BENUTZERHANDBUCH

CVE-30360

VERSION 1.3
FEBRUARY, 2012

STANDARD-ANMELDEDATEN	
IP-Adresse	192.168.0.1
Benutzername	admin
Passwort	password

HitronTechnologies

ÜBER DIESES BENUTZERHANDBUCH

WAS IN DIESEM BENUTZERHANDBUCH BESCHRIEBEN WIRD

In diesem Benutzerhandbuch wird beschrieben, wie die Funktionen des CVE-30360 über seine grafische Benutzeroberfläche konfiguriert werden.

VERWENDUNG DIESES BENUTZERHANDBUCHS

Dieses Handbuch beschreibt jede Eingabemaske des CVE-30360 sowie die Verwendung der unterschiedlichen Funktionen.

- In der Einführung (Seite 15) finden Sie eine Übersicht über die in diesem Handbuch beschriebenen Themen.
- Im Inhaltsverzeichnis (Seite 7), Abbildungsverzeichnis (Seite 11) und Tabellenverzeichnis (Seite 13) können Sie schnell die Informationen zu einer bestimmten Eingabemaske oder einem Thema finden.
- Im Index (Seite 81) erhalten Sie Informationen zu bestimmten Schlüsselwörtern.
- Im Rest des Benutzerhandbuchs erhalten Sie eine ausführliche Beschreibung der Funktionen des CVE-30360.

WEITERE DOKUMENTE

- **Installations-Kurzanleitung:** In dieser Anleitung wird kurz beschrieben, wie der CVE-30360 installiert wird. Sie enthält Informationen zu den Systemvoraussetzungen, zum Packungsinhalt, zur Installation und Hinweise zur Fehlerbehebung.
- **Online-Hilfe:** Jede Maske der Benutzeroberfläche des CVE-30360 verfügt über eine **Hilfe**-Taste. Wenn Sie auf diese Taste klicken, erhalten Sie zusätzliche Informationen zum Konfigurieren der Einstellungen.

ZUM GEBRAUCH DES BENUTZERHANDBUCHS

In diesem Benutzerhandbuch werden bestimmte Inhaltstypen mit bestimmten typographischen Merkmalen und Stilmerkmalen gekennzeichnet:

- Aufzählungen dienen dazu, verschiedene Einträge aufzulisten und auf Optionen hinzuweisen.

1. Nummerierte Absätze beschreiben die einzelnen Verfahrensschritte.

HINWEIS: Hinweise enthalten weiterführende Informationen zu einem Thema.

Warnungen enthalten Informationen zu Handlungsweisen, bei denen das Gerät beschädigt werden kann.

Produktbezeichnungen, Feldbezeichnungen, Auswahlfelder usw. sind **fett** geschrieben. Beispiel:

> Wählen Sie **UDP**, um das "User Datagram Protocol" zu verwenden.

Ein Mausklick in einer Eingabemaske ist durch eine spitze Klammer (>) gekennzeichnet. Beispiel:

> Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen**.

Das bedeutet, dass Sie in der Maske zunächst auf **Einstellungen** und dann auf **Erweiterte Einstellungen** klicken müssen.

Tasten werden mit Großbuchstaben in eckigen Klammern dargestellt. Beispiel:

> Drücken Sie zum Fortfahren auf [ENTER].

KUNDENBETREUUNG

Wenn Sie technische Hilfe benötigen oder andere Probleme auftreten, wenden Sie sich an Ihren Hitron-Vertreter.

Copyright © 2011 Hitron Technologies. Alle Rechte vorbehalten. Alle Marken und eingetragenen Marken sind das Eigentum der rechtmäßigen Eigentümer.

HAFTUNGSAUSSCHLUSS: Die in diesem Benutzerhandbuch enthaltenen Informationen sind zum Zeitpunkt der Druckstellung richtig. Dieses Benutzerhandbuch liegt in der vorliegenden Form vor und enthält keine ausdrücklichen oder impliziten Garantien/Gewährleistungen. Hitron Technologies und seine Vertreter übernehmen weder die Haftung für Ungenauigkeiten in diesem Benutzerhandbuch noch für Verluste, die durch die Beachtung oder Nicht-Beachtung der Anweisungen in diesem Benutzerhandbuch entstehen.

INHALTSVERZEICHNIS

Über dieses Benutzerhandbuch 3

Inhaltsverzeichnis 7

Abbildungsverzeichnis 11

Tabellenverzeichnis 13

Einführung 15

1.1 CVE-30360 Übersicht 15
1.1.1 Die wichtigsten Funktionen 16
1.2 Hardwareverbindungen 16
1.3 LEDs 18
1.4 Einrichten der IP-Adresse 20
1.4.1 Manuelles Einrichten der IP-Adresse 21
1.5 Anmelden beim CVE-30360 22
1.6 Übersicht über die Benutzeroberfläche 23
1.7 Zurücksetzen des CVE-30360 23

Kabel 25

2.1 Die Eingabemaske SYSTEM INFO 25
2.2 Die Eingabemaske Initialisierung 27
2.3 Die Eingabemaske Status 27
2.4 Die Eingabemaske Passwort 30

LAN 33

3.1 Übersicht über den Menüpunkt LAN 33
3.1.1 LAN-Netzwerke 33
3.1.2 LAN IP-Adressen und Subnetze 33

3.1.3 Domain-Suffix 34
3.1.4 Fehlersuche (Ping und Traceroute) 34
3.2 Die Eingabemaske LAN IP 34
3.3 Die Eingabemaske SWITCH SETUP 37
3.4 Die Eingabemaske DEBUG 37
3.5 Die Eingabemaske SICHERUNGSKOPIE 38

Firewall 41

4.1 Übersicht über den Menüpunkt Firewall 41
4.1.1 Firewall 41
4.1.2 Ping 41
4.1.3 MAC-Filter 41
4.1.4 IP-FILTERUNG 42
4.1.5 PORT FORWARDING 42
4.1.6 PORT TRIGGERING 42
4.2 Die Eingabemaske Firewall-Optionen 42
4.3 Die Eingabemaske MAC-Filter 44
4.4 Die Eingabemaske IP-FILTERUNG 46
4.4.1 Hinzufügen oder Bearbeiten einer IP-Filterregel 48
4.5 Die Eingabemaske FORWARDING 49
4.5.1 Hinzufügen oder Bearbeiten einer Portweiterleitungsregel 51
4.6 Die Eingabemaske PORT TRIGGERING 53
4.6.1 Hinzufügen oder Bearbeiten einer Port-Triggering-Regel 54

Wireless 57

5.1 Grundeinstellungen des Drahtlosnetzwerks 57
5.1.1 WLAN-Standards 58
5.1.2 Service Sets und SSIDs 58
5.1.3 Grundlagen für die WLAN-Sicherheit 59
5.2 Anleitung zur Nutzung der Drahtlosfunktion 59
5.2.1 Auswählen eines Sicherheitsverfahrens 59
5.2.2 Wechseln des Passworts für den Zugriff auf das Drahtlosnetzwerk . 60
5.2.3 Ändern des Netzwerknamens (SSID) 61
5.2.4 Verbergen des Netzwerks 61
5.2.5 Verbessern der Leistung des Drahtlosnetzwerks 61
5.3 Erweiterte Drahtlosnetzwerkfunktionen 62
5.3.1 Erweiterte Sicherheitseinstellungen im Drahtlosnetzwerk 62
5.3.2 Sonstige Informationen über Drahtlosnetzwerke 63
5.3.2.1 WPS 63
5.3.2.2 WMM 64

5.4 Die Eingabemasken für die Drahtloskonfiguration 64
5.4.1 DIE EINGABEMASKE WIRELESS-GRUNDEINSTELLUNGEN 64
5.4.2 Die Eingabemaske Sicherheit 66
5.4.3 DIE EINGABEMASKE ZUGANGS KONTROLLE 70
5.4.4 DIE EINGABEMASKE WI-FI SITE SURVEY 72

EMTA 75

6.1 Die Eingabemaske Status 75

Fehlerbehebung 77

Index 81

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1: Übersicht über die Funktionen 15
ABBILDUNG 2: Hardwareverbindungen 17
ABBILDUNG 3: LEDs 19
ABBILDUNG 4: Login 22
ABBILDUNG 5: Übersicht über die Benutzeroberfläche 23
ABBILDUNG 6: Die Eingabemaske Kabel > System Info 25
ABBILDUNG 7: Die Eingabemaske Kabel > Initialisierung 27
ABBILDUNG 8: Die Eingabemaske Kabel > Status 28
ABBILDUNG 9: Die Eingabemaske Kabel > Passwort 30
ABBILDUNG 10: Die Eingabemaske LAN > LAN IP 35
ABBILDUNG 11: Die Eingabemaske LAN > Switch Setup 37
ABBILDUNG 12: Die Eingabemaske LAN > Debug 38
ABBILDUNG 13: Die Eingabemaske LAN > Sicherungskopie 38
ABBILDUNG 14: Die Eingabemaske Firewall > Firewall-Optionen 43
ABBILDUNG 15: Die Eingabemaske Firewall > MAC-Filter 44
ABBILDUNG 16: Die Eingabemaske Firewall > IP-Filterung 47
ABBILDUNG 17: Die Eingabemaske Firewall > IP-Filterung > Hinzufügen/Bearbeiten 48
ABBILDUNG 18: Die Eingabemaske Firewall > Forwarding 50
ABBILDUNG 19: Die Eingabemaske Firewall > Forwarding > Hinzufügen/Bearbeiten 52
ABBILDUNG 20: Die Eingabemaske Firewall > Port Triggering 53
ABBILDUNG 21: Die Eingabemaske Firewall > Port Triggering > Hinzufügen/Bearbeiten 55
ABBILDUNG 22: Beispiel für ein Drahtlosnetzwerk 58
ABBILDUNG 23: Die Eingabemaske Wireless > Basic 64
ABBILDUNG 24: WPS PIN 65
ABBILDUNG 25: Die Eingabemaske Wireless > Sicherheit 67
ABBILDUNG 26: Wireless > Zugangs Kontrolle. 70
ABBILDUNG 27: Die Eingabemaske Wireless > Wi-Fi Site Survey 72
ABBILDUNG 28: Die Maske EMTA > Status 75

TABELLENVERZEICHNIS

TABELLE 1: Hardwareverbindungen 17
TABELLE 2: LEDs 19
TABELLE 3: Übersicht über die Benutzeroberfläche 23
TABELLE 4: Die Eingabemaske Kabel > System Info 26
TABELLE 5: Die Eingabemaske Kabel > Status 28
TABELLE 6: Die Eingabemaske Kabel > Passwort 30
TABELLE 7: Die Eingabemaske LAN > LAN IP 35
TABELLE 8: Die Eingabemaske LAN > Switch Setup 37
TABELLE 9: Die Eingabemaske LAN > Fehlersuche 38
TABELLE 10: Die Eingabemaske LAN > Sicherungskopie 39
TABELLE 11: Die Eingabemaske Firewall > Firewall-Optionen 43
TABELLE 12: Die Eingabemaske Firewall > MAC-Filter 45
TABELLE 13: Die Eingabemaske Firewall > IP-Filterung 47
TABELLE 14: Die Eingabemaske Firewall > IP-filterung > Hinzufügen/Bearbeiten ...49
TABELLE 15: Die Eingabemaske Firewall > Forwarding 50
TABELLE 16: Die Eingabemaske Firewall > Forwarding > Hinzufügen/Bearbeiten ..52
TABELLE 17: Die Eingabemaske Firewall > Port Triggering 53
TABELLE 18: Die Eingabemaske Firewall > Port Triggering > Hinzufügen/Bearbeiten 55
TABELLE 19: Die Eingabemaske Wireless > Basic 65
TABELLE 20: Die Eingabemaske Wireless > Sicherheit 67
TABELLE 21: Das Fenster Wireless > Zugangs Kontrolle 70
TABELLE 22: Die Eingabemaske Wireless > Wi-Fi Site Survey 72
TABELLE 23: Die Maske EMTA > Status 75

1

EINFÜHRUNG

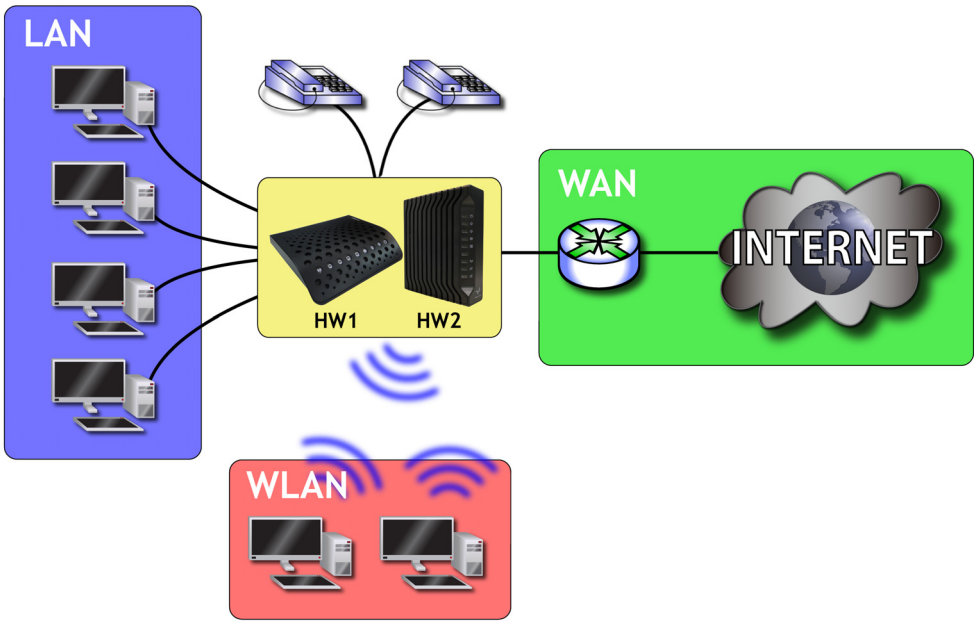
In diesem Kapitel erhalten Sie eine Übersicht über den CVE-30360 und eine Einführung in seine Benutzeroberfläche.

1.1 CVE-30360 ÜBERSICHT

Der CVE-30360 ist gleichzeitig ein Kabelmodem und ein drahtloser Zugangspunkt (AP). An das Gerät können Sie Ihre Computer, analogen Telefone, Drahtlosgeräte und anderen Netzwerkgeräte anschließen, um sie miteinander und über die Kabelverbindung mit dem Internet zu verbinden.

Computer, die über ein Kabel mit dem CVE-30360 verbunden sind, befinden sich im lokalen Netzwerk, dem LAN. Computer, die drahtlos mit dem CVE-30360 verbunden sind, befinden sich im drahtlosen lokalen Netzwerk, dem WLAN. Der CVE-30360 stellt wiederum die Verbindung zum Internetdienstanbieter über das Weitbereichsnetzwerk, dem WAN, her.

ABBILDUNG 1: Übersicht über die Funktionen



1.1.1 DIE WICHTIGSTEN FUNKTIONEN

Der CVE-30360 bietet:

- Internetverbindung zum Kabelmodemdienst über den **CATV**-Port (HF-Anschluss Typ F)
- Voice-Verbindung zum Telefoniedienstanbieter.
- LAN-Verbindung über vier Ethernet-Ports mit einer Verbindungsgeschwindigkeit von 10/100/1000 Mbps (Megabits pro Sekunde)
- DHCP-Protokoll (Dynamic Host Configuration Protocol) für Geräte im LAN/WLAN
- LAN-Fehlerbehebungstools (Ping und Traceroute)
- IEEE 802.11b/g/n drahtloses MIMO-Networking (Multiple-In, Multiple-Out) mit Geschwindigkeiten von bis zu 300 Mbps
- Sicherheit bei der Drahtlosverbindung: WEP-, WPA-PSK- und WPA2-PSK-Verschlüsselung, Wifi Protected Setup (WPS), Push-Button- und PIN-Konfiguration sowie MAC-Filter
- Sicherheit bei der Kabelverbindung: Stateful-Inspection-Firewall, IP- und MAC-Filter, Portweiterleitung und Port-Triggering
- Sichern und Wiederherstellen von Einstellungen
- Sichere Konfigurationsschnittstelle, zugänglich über Webbrowser

1.2 HARDWAREVERBINDUNGEN

In diesem Abschnitt werden die Ports und Tasten des CVE-30360 beschrieben.

ABBILDUNG 2: Hardwareverbindungen

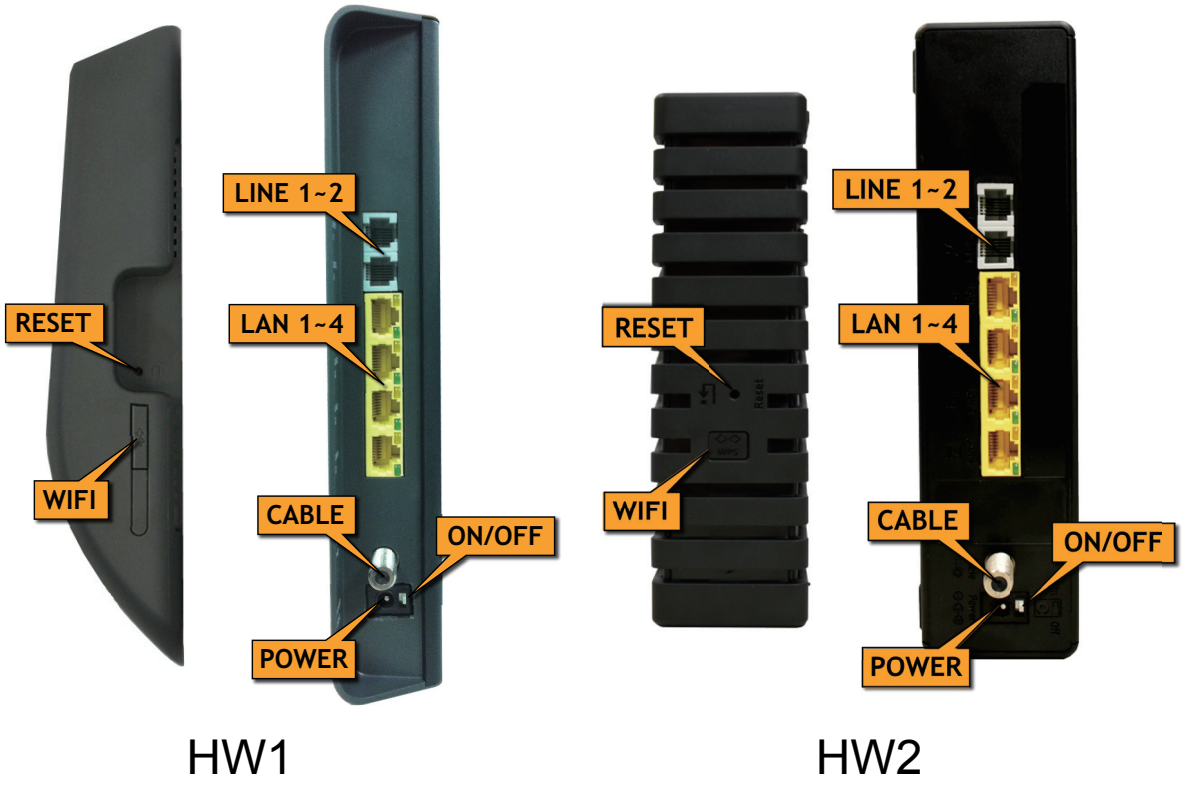


TABELLE 1: Hardwareverbindungen

WIFI	Mit dieser Taste können Sie das Drahtlosnetzwerk ein- oder ausschalten und die WPS PBC-Prozedur starten (weitere Informationen finden Sie unter WPS auf Seite 63). ▶ Drücken Sie 1 bis 5 Sekunden lang auf diese Taste, um das Drahtlosnetzwerk ein- oder auszuschalten. ▶ Um die WPS PBC-Verbindungsprozedur zu starten, müssen Sie 5 bis 10 Sekunden lang auf diese Taste drücken. Drücken Sie innerhalb der folgenden 2 Minuten auf die PBC-Tasten der Drahtlosgeräte, die sich innerhalb der Sendereichweite befinden, um sie zum Drahtlosnetzwerk hinzuzufügen.
Reset	Mit dieser Taste können Sie den CVE-30360 neu starten oder zurücksetzen. ▶ Drücken Sie auf diese Taste, und halten Sie sie kurz gedrückt, um den CVE-30360 neu zu starten. Der CVE-30360 wird mit den bestehenden Einstellungen neu gestartet. ▶ Drücken Sie auf diese Taste, und halten Sie sie länger als 10 Sekunden lang gedrückt, um alle benutzerdefinierten Einstellungen zurückzusetzen und den CVE-30360 mit den Standardeinstellungen neu zu starten.

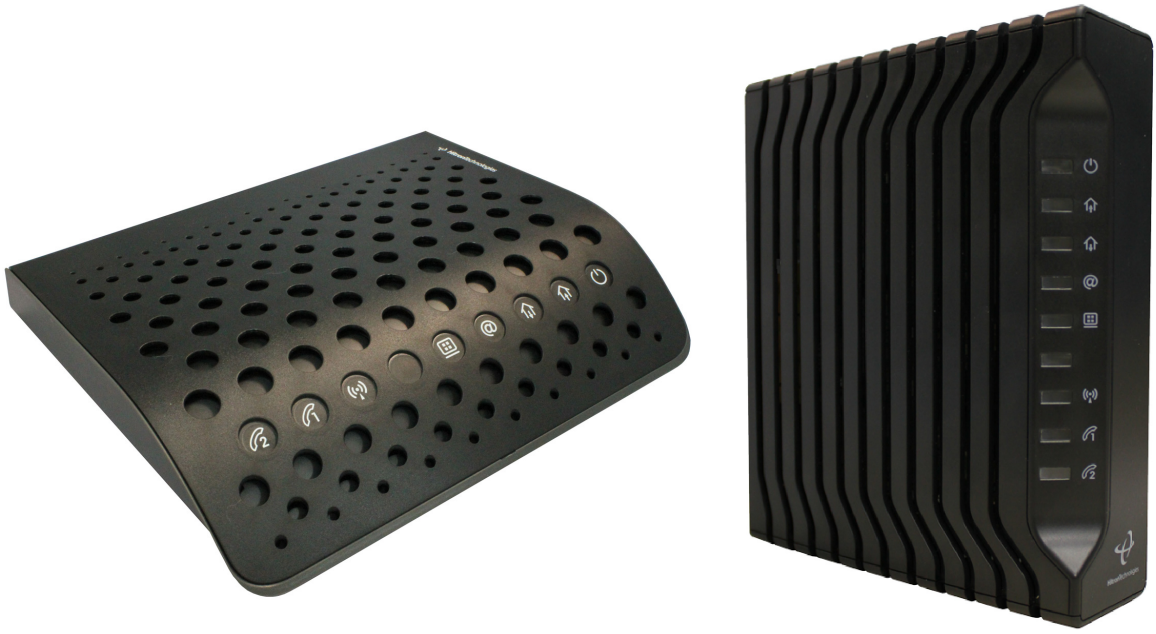
TABELLE 1: Hardwareverbindungen

LAN1	An diese Ports werden Ihr Computer und andere Netzwerkgeräte angeschlossen. Verwenden Sie dazu Ethernet-Kabel der Kategorie 5 oder 6 mit RJ45-Stecker.
LAN2	
LAN3	
LAN4	
LINE 1	An diese Ports werden Ihre Analogtelefone für VoIP-Dienste angeschlossen. Verwenden Sie dazu Kabel mit RJ11-Stecker.
LINE 2	
CABLE	Hier schließen Sie ein HF-Kabel Typ F für die Verbindung mit dem Internet an.
POWER	Hier schließen Sie den 12 V/2 A-Netzadapter an, der im Lieferumfang des CVE-30360 enthalten ist. **Verwenden Sie NIEMALS einen anderen Netzadapter für die Stromversorgung des CVE-30360. Anderenfalls kann der CVE-30360 beschädigt werden.**
ON/OFF	Mit diesem Schalter können Sie den CVE-30360 ein- oder ausschalten. - Um den CVE-30360 einzuschalten, schieben Sie den Schalter in die Position ON. - Um den CVE-30360 auszuschalten, schieben Sie den Schalter in die Position OFF.

1.3 LEDS

In diesem Abschnitt werden die LED-Lampen des CVE-30360 beschrieben.

ABBILDUNG 3: LEDs



HW1 HW2

TABELLE 2: LEDs

LED	STATUS	**BESCHREIBUNG**
LINE 1 LINE 2	Leuchtet nicht	Ihr Tarif umfasst nicht den Telefoniedienst. ***HINWEIS:*** Die Anzahl der leuchtenden **LINE**-LEDs ist abhängig von dem von Ihnen gewählten Tarif.
	Blinkt	An den entsprechenden **Line**-Port ist ein Telefon angeschlossen, und der Hörer ist abgehoben.
	Leuchtet	Ihr Tarif umfasst den Telefoniedienst. ***HINWEIS:*** Die Anzahl der leuchtenden **LINE**-LEDs ist abhängig von dem von Ihnen gewählten Tarif.
WIRELESS	Leuchtet nicht	Über das Drahtlosnetzwerk werden Daten weder gesendet noch empfangen.
	Blinkt	Über das Drahtlosnetzwerk werden Daten gesendet oder empfangen.
ETH	Leuchtet nicht	Es sind keine Geräte an den **LAN**-Ports angeschlossen.
	Blinkt	Ein Gerät ist über eine Fast-Ethernet-Verbindung an einen **LAN**-Port angeschlossen, und es werden Daten gesendet oder empfangen.
	Leuchtet	Ein Gerät ist über eine Fast-Ethernet-Verbindung an einen **LAN**-Port angeschlossen, es werden aber keine Daten gesendet oder empfangen.

TABELLE 2: LEDs

Status	Blinkt	Das Kabelmodem des CVE-30360 registriert sich gerade beim Dienstanbieter.
	Leuchtet	Das Kabelmodem des CVE-30360 hat sich erfolgreich beim Dienstanbieter registriert.
US	Blinkt	Der CVE-30360 sucht gerade nach einer Upstream-Frequenz in der **CATV**-Verbindung.
	Leuchtet	Der CVE-30360 hat erfolgreich eine Upstream-Frequenz in der **CATV**-Verbindung gefunden und sich festgelegt.
DS	Blinkt	Der CVE-30360 sucht gerade nach einer Downstream-Frequenz in der **CATV**-Verbindung.
	Leuchtet	Der CVE-30360 hat erfolgreich eine Downstream-Frequenz in der **CATV**-Verbindung gefunden und sich festgelegt.
Power	Leuchtet	Der CVE-30360 wird mit Strom versorgt.
	Leuchtet nicht	Der CVE-30360 wird nicht mit Strom versorgt.

Wenn Sie den CVE-30360 einschalten, beginnen die LEDs in der folgenden Reihenfolge zu leuchten:

- **Power**
- **US**
- **DS**
- **Status**
- Die LEDs **ETH 1-4** leuchten, sobald an den entsprechenden Ports Aktivität ermittelt wird, die LEDs **LINE 1-2** leuchten, wenn Ihr Dienstvertrag auch Telefonie umfasst (die Anzahl der leuchtenden LEDs ist abhängig von Ihrem Tarif). Die **WIRELESS**-LED leuchtet, sobald das Drahtlosnetzwerk bereit ist.

1.4 EINRICHTEN DER IP-ADRESSE

Wenn Sie die Benutzeroberfläche des CVE-30360 aufrufen möchten, müssen sich die IP-Adresse des Computers und die des CVE-30360 im selben Subnetz befinden. Nur so ist die Kommunikation des Computers mit dem CVE-30360 möglich.

Der CVE-30360 verfügt über einen integrierten DHCP-Server. Sobald er aktiviert ist, kann er Computern im LAN IP-Adressen zuweisen. Wenn der DHCP-Server aktiv ist, können Sie automatisch eine IP-Adresse beziehen. Der DHCP-Server ist standardmäßig aktiviert.

Wenn Ihr Computer so konfiguriert ist, dass er eine IP-Adresse automatisch beziehen kann, oder wenn Sie das nicht genau wissen, versuchen Sie zunächst, sich beim CVE-30360 anzumelden (siehe Anmelden beim CVE-30360 auf Seite 22).

- Wenn die Anmeldemaske erscheint, ist der Computer bereits richtig konfiguriert.

- Wenn die Anmeldemaske nicht erscheint, ist entweder der DHCP-Server des CVE-30360 nicht aktiviert, oder der Computer ist nicht richtig konfiguriert. Folgen Sie der Anweisung gemäß Manuelles Einrichten der IP-Adresse auf Seite 21, und richten Sie den Computer so ein, dass er eine IP-Adresse automatisch bezieht. Versuchen Sie erneut, sich anzumelden. Wenn Sie sich nicht anmelden können, richten Sie wie unten beschrieben noch einmal manuell eine IP-Adresse ein. Versuchen Sie erneut, sich anzumelden.

HINWEIS: Wenn die Anmeldemaske weiterhin nicht angezeigt wird, wurden möglicherweise die Einstellungen des CVE-30360 geändert. Wenn Sie die neue Adresse des CVE-30360 nicht kennen, sollten Sie die Standardeinstellungen wiederherstellen. Siehe Zurücksetzen des CVE-30360 auf Seite 23. Beachten Sie, dass dabei ALLE benutzerdefinierten Einstellungen verloren gehen.

1.4.1 MANUELLES EINRICHTEN DER IP-ADRESSE

Standardmäßig ist die lokale IP-Adresse des CVE-30360 **192.168.0.1 (http://hitronhub.home)**. Wenn der CVE-30360 die IP-Standardadresse verwendet, muss die IP-Adresse des Computers zwischen **192.168.0.2** und **192.168.0.254** liegen.

HINWEIS: Wenn der DHCP-Server des CVE-30360 aktiviert ist, richten Sie den Computer so ein, dass er bei Schritt 5 automatisch eine IP-Adresse bezieht. Der CVE-30360 weist dann dem Computer eine IP-Adresse zu. Der DHCP-Server ist standardmäßig aktiviert.

Führen Sie die folgenden Schritte aus, um die IP-Adresse Ihres Computers für die Verbindung mit dem CVE-30360 manuell einzurichten:

HINWEIS: Bei diesem Beispiel wird die Installation unter dem Betriebssystem Windows XP ausgeführt. Bei anderen Betriebssystemen kann das Verfahren abweichen.

1. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
2. Klicken Sie in dem nun angezeigten Fenster doppelt auf **Netzwerkverbindungen**.
3. Klicken Sie mit der rechten Maustaste auf Ihre Netzwerkverbindungsart (normalerweise **LAN-Verbindung**), und klicken Sie dann auf **Eigenschaften**.
4. Scrollen Sie in der Liste **Diese Verbindung verwendet folgende Elemente**: auf der Registerkarte **Allgemein** nach unten, und wählen Sie **Internetprotokoll (TCP/IP)**. Klicken Sie auf **Eigenschaften**.
5. Sie können eine IP-Adresse automatisch beziehen oder manuell festlegen:
   - Wenn der DHCP-Server des CVE-30360 aktiviert ist, wählen Sie die Option **IP-Adresse automatisch beziehen**.
   - Wenn der DHCP-Server des CVE-30360 nicht aktiviert ist, wählen Sie die Option **Folgende IP-Adresse verwenden**. Geben Sie in das Feld **IP-Adresse** eine Adresse zwischen **192.168.0.2** und **192.168.0.254** (Standard) ein. Geben Sie in das Feld **Subnetzmaske 255.255.255.0** (Standard) ein.

HINWEIS: Wenn der CVE-30360 nicht die IP-Standardadresse verwendet, wählen Sie die IP-Adresse und Subnetzmaske so, dass der Computer im selben Subnetz liegt wie der CVE-30360.

6 Klicken Sie auf **OK**. Das Fenster **Internetprotokoll (TCP/IP)** schließt sich. Klicken Sie im Fenster **LAN-Verbindungseigenschaften** auf **OK**.

Der Computer erhält jetzt eine IP-Adresse vom CVE-30360 zugewiesen oder er verwendet die von Ihnen festgelegte IP-Adresse. Er kann dann mit dem CVE-30360 kommunizieren.

1.5 ANMELDEN BEIM CVE-30360

Führen Sie die folgenden Schritte aus, um sich beim CVE-30360 anzumelden und die Benutzeroberfläche aufzurufen.

HINWEIS: Sie können sich zwar über die Drahtlosschnittstelle beim CVE-30360 anmelden, es wird aber empfohlen, den CVE-30360 über eine Kabelverbindung mit dem LAN zu konfigurieren.

1 Öffnen Sie ein Browserfenster.

2 Geben Sie in die Adresszeile des Browsers die IP-Adresse des CVE-30360 ein (Standard **192.168.0.1**). Die Eingabemaske **Anmelden** erscheint.

ABBILDUNG 4: Login

3 Geben Sie den **Benutzernamen** und das **Passwort** ein. Der Anmeldebenutzername ist standardmäßig **admin**, das Anmeldepasswort ist **password**.

HINWEIS: Beachten Sie bei der Eingabe des Benutzernamens und Passworts die Groß- und Kleinschreibung - “admin” ist nicht dasselbe wie “Admin”.

4 Klicken Sie auf **Login**. Die Maske **System Info** wird angezeigt (siehe Die Eingabemaske SYSTEM INFO auf Seite 25).

1.6 ÜBERSICHT ÜBER DIE BENUTZEROBERFLÄCHE

In diesem Abschnitt wird die Benutzeroberfläche des CVE-30360 beschrieben.

ABBILDUNG 5: Übersicht über die Benutzeroberfläche

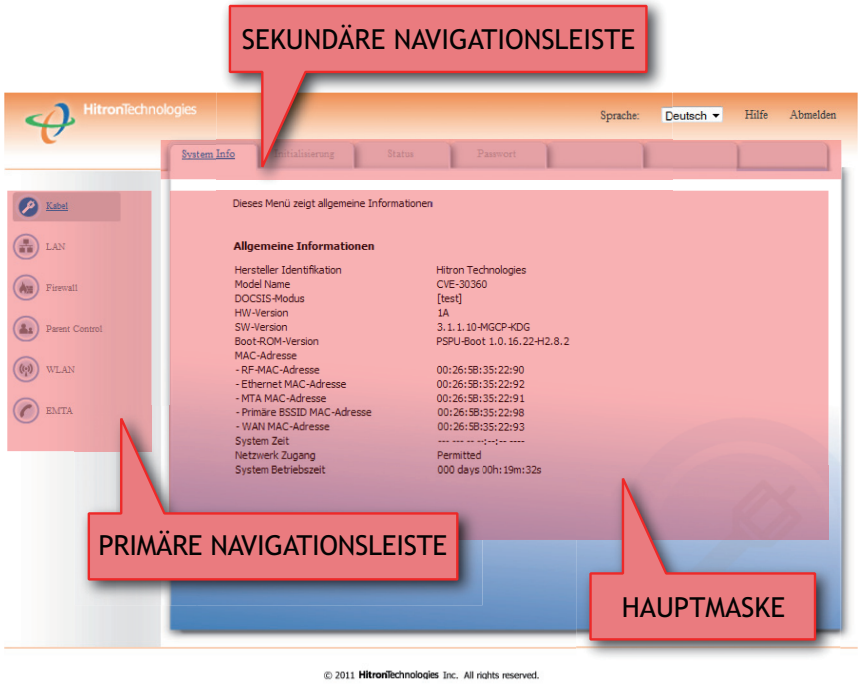


TABELLE 3: Übersicht über die Benutzeroberfläche

Primäre Navigationsleiste	In diesem Bereich können Sie von einem Bereich der Benutzeroberfläche zu einem anderen Bereich wechseln.
Sekundäre Navigationsleiste	In diesem Bereich können Sie von einer Eingabemaske zu einer anderen wechseln.
Hauptmaske	In diesem Bereich finden Sie Informationen zur Konfiguration des CVE-30360, und hier können Sie die Konfigurationen ändern.

1.7 ZURÜCKSETZEN DES CVE-30360

Wenn Sie die Standardeinstellungen des CVE-30360 wiederherstellen, gehen alle benutzerdefinierten Einstellungen verloren, und der CVE-30360 wird auf seinen ursprünglichen Konfigurationsstatus zurückgesetzt.

Der CVE-30360 kann auf zwei Arten zurückgesetzt werden:

- Drücken Sie auf die **RESET**-Taste des CVE-30360, und halten Sie diese mindestens 10 Sekunden lang gedrückt.
- Klicken Sie auf **LAN** > **Sichern**. Klicken Sie in der folgenden Maske auf die Schaltfläche **Zurücksetzen auf Werkseinstellungen**.

Der CVE-30360 schaltet sich aus und mit den Standardeinstellungen wieder ein.

HINWEIS: Entsprechend der vorherigen Konfiguration des CVE-30360 müssen eventuell die IP-Einstellungen des Computers neu konfiguriert werden (siehe Einrichten der IP-Adresse auf Seite 20).

2 KABEL

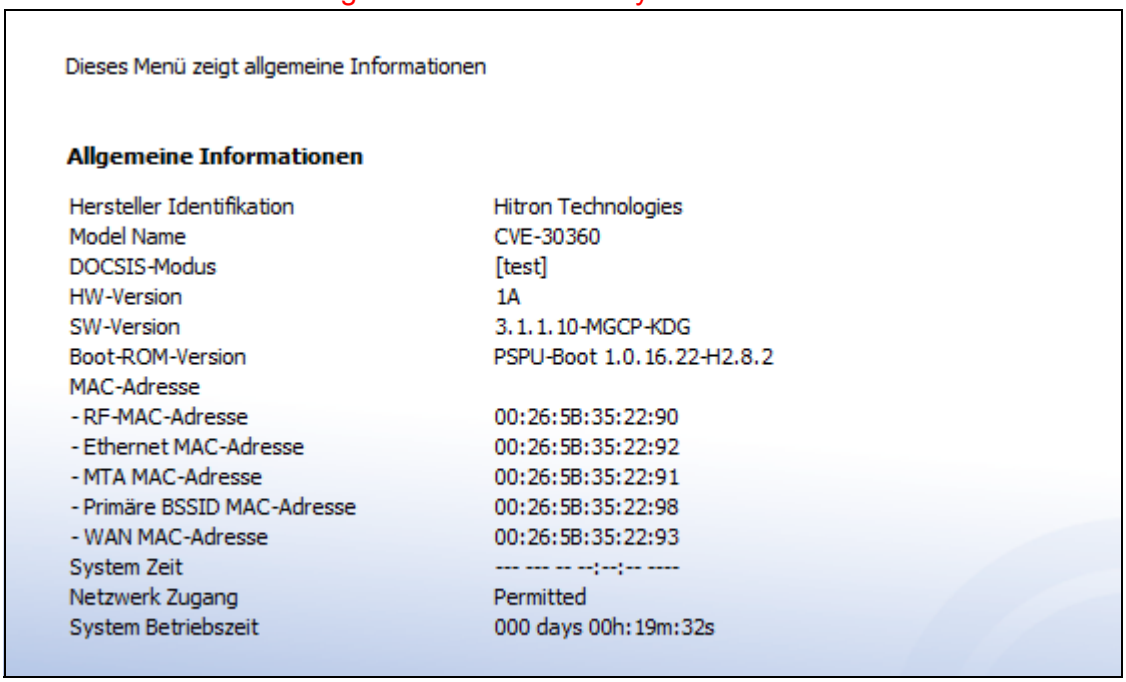
2.1 DIE EINGABEMASKE SYSTEM INFO

In dieser Eingabemaske werden allgemeine Informationen zur Hardware und Software des CVE-30360 sowie zur Internetverbindung angezeigt.

HINWEIS: Die meisten hier angezeigten Informationen benötigen Sie nur im Falle einer Fehlerbehebung. Hier finden Sie u. a. auch Informationen zur MAC-Adresse, die Sie zum Einrichten des Netzwerks benötigen.

Klicken Sie auf **Kabel** > **System Info**. Die folgende Eingabemaske erscheint.

ABBILDUNG 6: Die Eingabemaske Kabel > System Info



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 4: Die Eingabemaske Kabel > System Info

Allgemeine Informationen	
Hersteller Identifikation	Hier wird der Name des Herstellers des CVE-30360 angezeigt.
Model Name	Hier wird der Gerätemodellname angezeigt (CVE-30360).
DOCSIS-Modus	Hier wird die Version des DOCSIS-Standards angezeigt, dem der CVE-30360 entspricht.
HW-Version	Hier wird die Versionsnummer der Hardware des CVE-30360 angezeigt.
SW-Version	Hier wird die Versionsnummer der Software des CVE-30360 angezeigt.
Boot-ROM-Version	Hier wird die Versionsnummer des Programms angezeigt, die den Bootvorgang (während die Hauptsoftware geladen wird) des CVE-30360 steuert.
MAC-Adresse	
RF-MAC-Adresse	Hier wird die MAC-Adresse des RF-Moduls des CVE-30360 angezeigt. Mit diesem Modul wird bei der **CATV**-Verbindung die Verbindung zum Internet hergestellt.
Ethernet MAC-Adresse	Hier wird die MAC-Adresse des Ethernet-Moduls des CVE-30360 angezeigt. Über dieses Modul werden die **LAN**-Ports angeschlossen.
MTA MAC-Adresse (im Routing-Modus)	Hier wird die MAC-Adresse des Moduls angezeigt, das bei einer **CATV**-Verbindung die Verbindung zum Internet herstellt, wenn sich der CVE-30360 im Routing-Modus befindet.
Primäre BSSID MAC-Adresse	Hier wird die MAC-Adresse der BSSID des CVE-30360 angezeigt. Es ist die MAC-Adresse des WLAN-Moduls, zu dem die Wireless Clients die Verbindung herstellen. ***HINWEIS:*** Je nach Vertragsumfang mit Ihrem Netzbetreiber können Sie auch weitere BSSIDs haben.
System Zeit	Hier werden das aktuelle Datum und die Uhrzeit angezeigt.
System Betriebszeit	Hier wird die Dauer in Tagen, Stunden, Minuten und Sekunden seit dem letzten Einschalten oder Neustart des CVE-30360 angezeigt.
Netzwerk Zugang	Hier wird angezeigt, wenn Sie mit Ihrem Internetdienstanbieter verbunden sind, und Sie können hier erkennen, ob der Internetdienstanbieter Ihnen den Zugriff auf das Internet über die **CATV**-Verbindung erlaubt. ▲ Wenn Sie auf das Internet zugreifen können, erscheint **Permitted**. ▲ Wenn Sie nicht auf das Internet zugreifen können, erscheint **Denied**.

2.2 DIE EINGABEMASKE INITIALISIERUNG

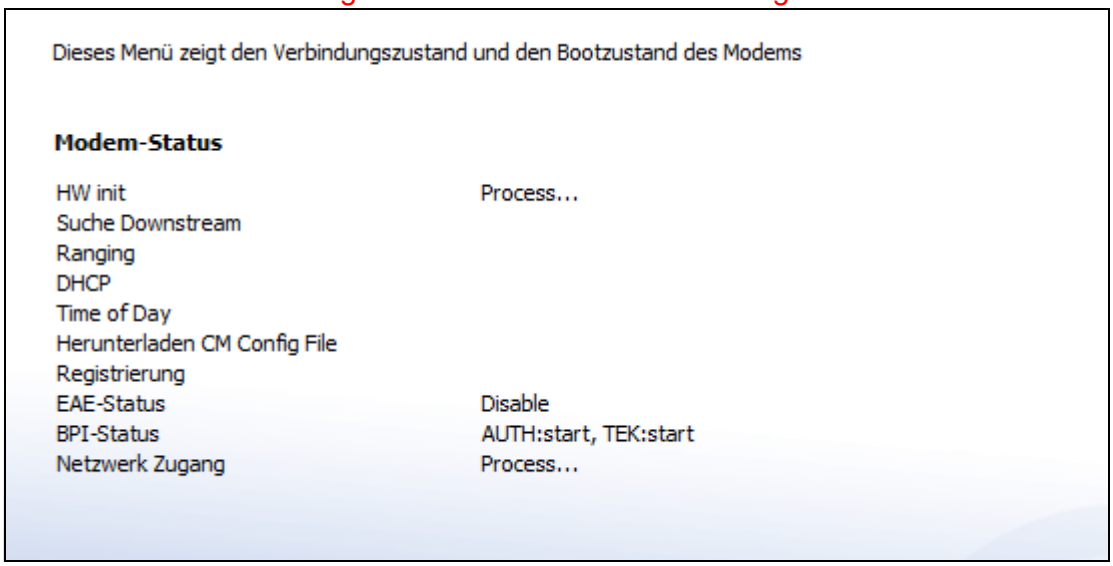
In dieser Eingabemaske werden die Schritte für die erfolgreiche **CATV**-Verbindung zum Internet angezeigt.

Diese Eingabemaske können Sie verwenden, um eventuelle Fehler zu beheben und um sicherzustellen, dass der CVE-30360 erfolgreich mit dem Internet verbunden wurde. Wenn keine Verbindung zustandegekommen ist, können Sie genau feststellen, bei welchem Schritt ein Fehler aufgetreten ist.

HINWEIS: Diese Eingabemaske erscheint, wenn Sie sich das erste Mal beim CVE-30360 anmelden.

Klicken Sie auf **Kabel** > **Initialisierung**. Die folgende Eingabemaske erscheint.

ABBILDUNG 7: Die Eingabemaske Kabel > Initialisierung



Bei jedem Schritt

- erscheint **Process...**, wenn der CVE-30360 versucht, eine Verbindung herzustellen.
- **Success**, wenn der CVE-30360 eine Verbindung erfolgreich hergestellt hat.

2.3 DIE EINGABEMASKE STATUS

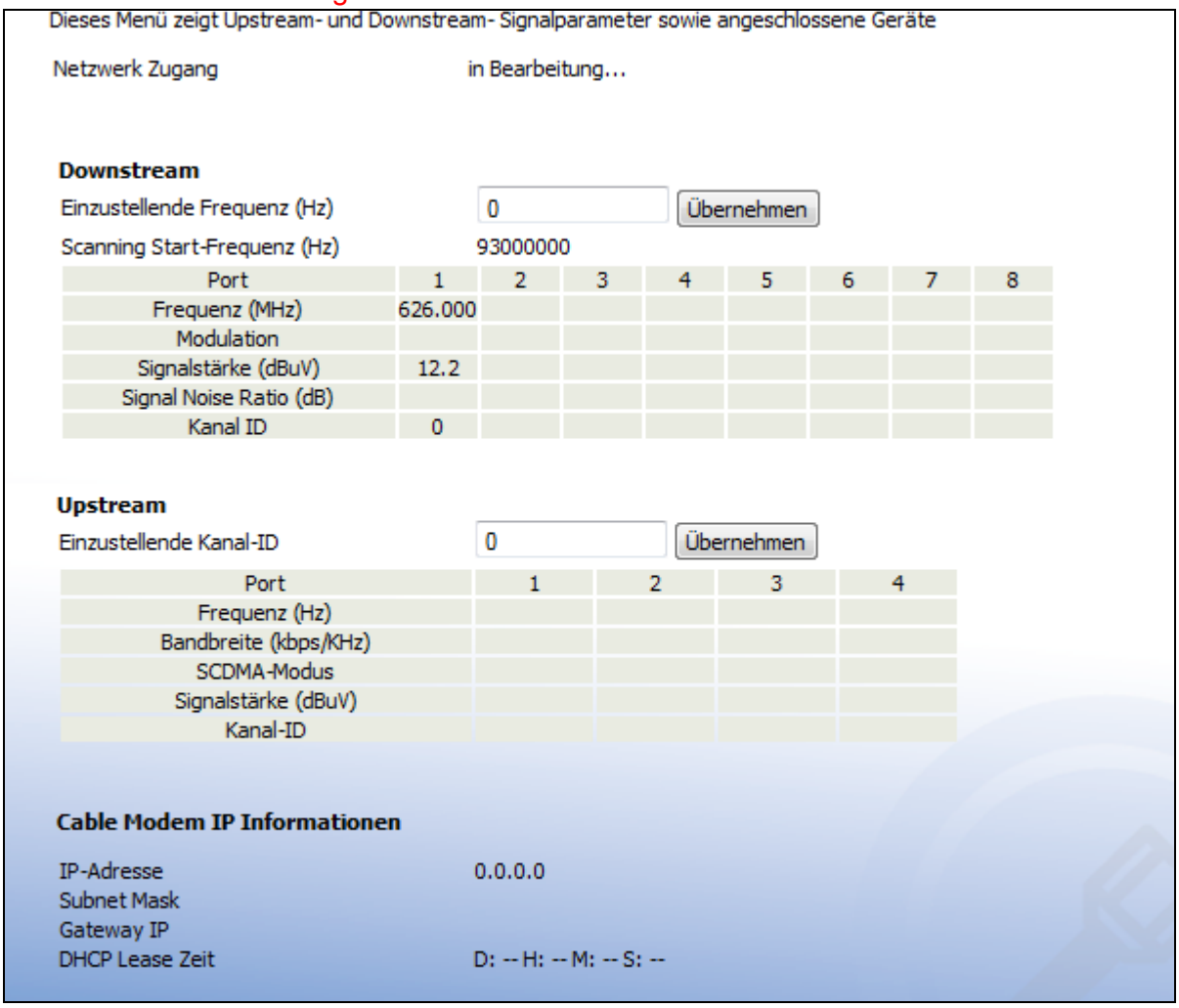
Auf dieser Eingabemaske erhalten Sie die folgenden Informationen:

- Die Art der Upstream- und Downstreamverbindung zwischen dem CVE-30360 und dem Gerät, mit dem er über die **CATV**-Schnittstelle verbunden ist.
- IP-Informationen der WAN-Verbindung des CVE-30360.

Sie können auch die Downstream-Mittenfrequenz des CVE-30360 konfigurieren.

Klicken Sie auf **Kabel** > **Status**. Die folgende Eingabemaske erscheint.

ABBILDUNG 8: Die Eingabemaske Kabel > Status



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 5: Die Eingabemaske Kabel > Status

Netzwerk Zugang	Hier wird angezeigt, ob der Internetdienstanbieter den Zugriff auf das Internet über die **CATV**-Verbindung zulässt. ▶ Wenn Sie auf das Internet zugreifen können, erscheint **Permitted**. ▶ Wenn Sie nicht auf das Internet zugreifen können, erscheint **Denied**.
Downstream ***HINWEIS:*** Das Downstream-Signal ist das zum CVE-30360 gesendete Signal.	

TABELLE 5: Die Eingabemaske Kabel > Status (Fortsetzung)

Einzustellende Frequenz	Hier wird die aktuelle Mittenfrequenz in Hertz (Hz) angezeigt, über die die Daten über die **CATV**-Schnittstelle zum CVE-30360 gesendet werden. Auf diese Frequenz ist der CVE-30360 so lange festgelegt, bis diese Frequenz nicht mehr verfügbar ist. Wenn Sie möchten, dass sich der CVE-30360 mit einer anderen Frequenz verbindet, geben Sie diese in dieses Feld ein, und klicken Sie auf **Übernehmen**. ***HINWEIS:*** Die Frequenz sollte aber nur geändert werden, wenn es unbedingt nötig ist.
Scanning Start-Frequenz	Hier wird die Frequenz in Hertz (Hz) angezeigt, bei der der CVE-30360 beginnt, nach einer Verbindung über die **CATV**-Schnittstelle zu suchen (wenn nicht bereits eine Frequenz festgelegt ist).
Frequenz	Hier wird die gerade verwendete Frequenz aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Modulation	Hier wird der Modulationstyp angezeigt, den jeder Downstream-Kanal verwendet.
Signalstärke	Hier wird die Signalstärke (in dBmV) aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Signal Noise Ratio	Hier wird das Signal-Rausch-Verhältnis (in dB) aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Upstream ***HINWEIS:*** Das Upstream-Signal ist das vom CVE-30360 gesendete Signal.	
Kanal-ID	Hier wird die ID aller Kanäle angezeigt, über die das Upstream-Signal übertragen wird.
Frequenz	Hier wird die Frequenz (in Hz) aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Bandbreite	Hier wird die Bandbreite (in Hz) aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
SCDMA-Modus	Hier wird der SCDMA-Modus aller Kanäle angezeigt, auf denen das Upstream-Signal übertragen wird.
Signalstärke	Hier wird die Signalstärke (in dBmV) aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Cable Modem IP Informationen	
IP-Adresse	Hier wird die WAN IP-Adresse des CVE-30360 angezeigt. Diese IP-Adresse wird demCVE-30360 automatisch zugewiesen.
Subnet Mask	Hier wird die WAN-Subnetzmaske des CVE-30360 angezeigt.

TABELLE 5: Die Eingabemaske Kabel > Status (Fortsetzung)

Gateway IP	Hier wird die IP-Adresse des Geräts angezeigt, mit dem der CVE-30360 über die **CATV**-Schnittstelle verbunden ist.
DHCP Lease Zeit	Hier wird angezeigt, wann die IP-Adresse des Geräts ungültig wird und ihm eine neue IP-Adresse vom DHCP-Server zugewiesen wird.
System Zeit	Hier werden das aktuelle Datum und die Uhrzeit angezeigt.

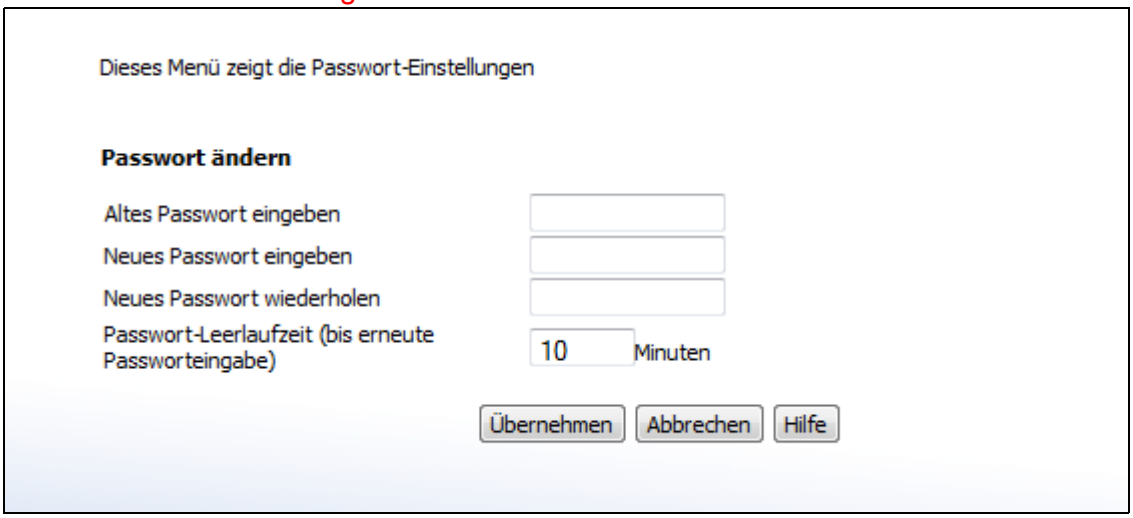
2.4 DIE EINGABEMASKE PASSWORT

Auf dieser Eingabemaske können Sie das Passwort ändern, mit dem Sie sich beim CVE-30360 anmelden.

HINWEIS: Sollten Sie das Passwort vergessen haben, müssen Sie den CVE-30360 auf seine Standardeinstellungen zurücksetzen.

Klicken Sie auf **Kabel** > **Passwort**. Die folgende Eingabemaske erscheint.

ABBILDUNG 9: Die Eingabemaske Kabel > Passwort



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 6: Die Eingabemaske Kabel > Passwort

Altes Passwort eingeben	Geben Sie das Passwort ein, mit dem Sie sich aktuell beim CVE-30360 anmelden müssen.
Neues Passwort eingeben	Geben Sie das neue Passwort für die Anmeldung beim CVE-30360 ein.
Neues Passwort wiederholen	
Passwort-Leerlaufzeit (bis erneute Passworteingabe)	Geben Sie hier die Anzahl der Leerlauf-Minuten ein, nach der sich der CVE-30360 automatisch abmeldet. Sobald diese Zeit abgelaufen ist, müssen Sie sich erneut anmelden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.

TABELLE 6: Die Eingabemaske Kabel > Passwort (Fortsetzung)

Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

3 LAN

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **LAN** klicken.

3.1 ÜBERSICHT ÜBER DEN MENÜPUNKT LAN

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **LAN** beschrieben.

3.1.1 LAN-NETZWERKE

Ein LAN-Netzwerk (Local Area Network) ist ein Netzwerk von Computern und anderen Geräten, das normalerweise einen kleinen begrenzten Bereich (z. B. ein Gebäude) abdeckt. Das LAN des CVE-30360 besteht aus allen Computern und Netzwerkgeräten, die an die Ports **LAN 1**-**4** angeschlossen sind. Es ist Ihr privates Netzwerk.

Das LAN ist ein vom WAN (Wide Area Network) abgetrenntes Netzwerk. Für den CVE-30360 umfasst das WAN alle Computer und sonstigen Geräte, die in der Kabelverbindung (**CATV**) verfügbar sind.

Standardmäßig können Computer des WAN nicht einzelne Computer eines LAN identifizieren. Sie erkennen nur den CVE-30360. Der CVE-30360 wickelt das Routing von und zu den einzelnen Computern im LAN ab.

3.1.2 LAN IP-ADRESSEN UND SUBNETZE

IP-Adressen im LAN werden entweder vom DHCP-Server des CVE-30360 gesteuert oder von Ihnen selbst festgelegt, wenn Sie Ihren Computern manuell IP-Adressen zuweisen.

3.1.3 DOMAIN-SUFFIX

Eine Domain ist eine Position in einem Netzwerk, z. B. **example.com**. Im Internet werden die IP-Adressen in der Form eines Domainnamens entsprechend des Domainnamensystems umgesetzt. Dadurch gelangen Sie bei Eingabe von “www.example.com” in den Browser auch dann zur entsprechenden Position im Internet, wenn sich die IP-Adresse des Website-Servers geändert hat.

Ähnlich haben Sie auch beim CVE-30360 die Möglichkeit, einen **Domain-Suffix** für das LAN festzulegen. Wenn Sie den Domain-Suffix in den Browser eingeben, erreichen Sie den CVE-30360 unabhängig von seiner IP-Adresse im LAN.

3.1.4 FEHLERSUCHE (PING UND TRACEROUTE)

Der CVE-30360 verfügt über einige Tools, mit denen Sie eine Netzwerkdiagnose im LAN durchführen können:

- Ping: Bei diesem Tool können Sie eine IP-Adresse eingeben und prüfen, ob ein Computer (oder ein anderes Netzwerkgerät) mit dieser Adresse im Netzwerk reagiert. Die Bezeichnung ist abgeleitet vom Impuls, den ein Unterwasserschallgerät aussendet, wenn es nach Objekten unter Wasser sucht. Beim Ping wird ähnlich vorgegangen. Mit diesem Tool können Sie feststellen, ob eine IP-Adresse genutzt wird oder ob ein Gerät (dessen IP-Adresse Sie kennen) richtig funktioniert.
- Traceroute: Mit diesem Tool können Sie nachverfolgen, welchen Weg bestimmte Datenpakete genommen haben, um vom CVE-30360 zum festgelegten Ziel zu gelangen. Mit diesem Tool können Sie Routing-Probleme lösen oder Firewalls erkennen, die den Zugriff auf einen Computer oder Dienst blockieren.

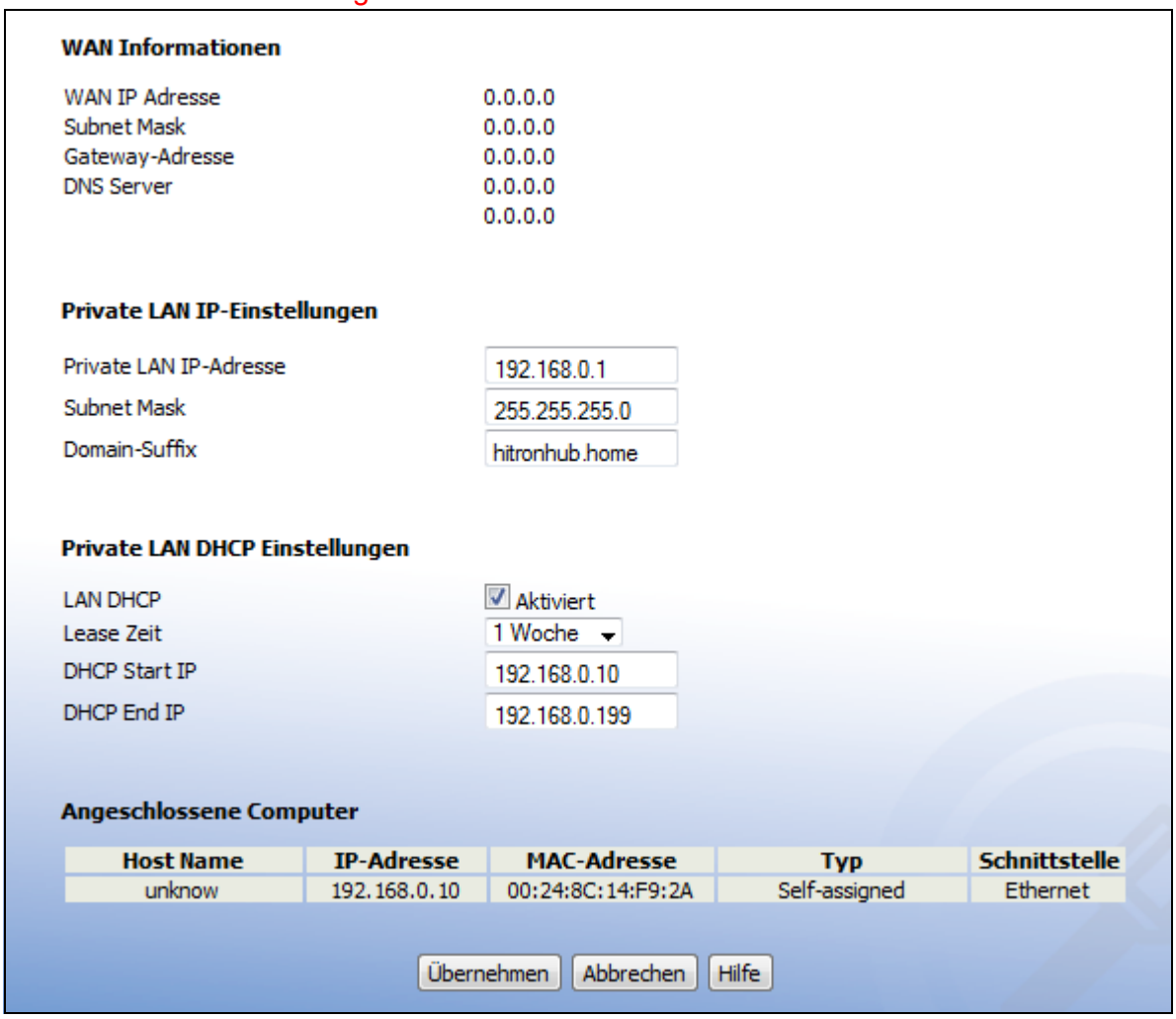
3.2 DIE EINGABEMASKE LAN IP

In dieser Maske können Sie Folgendes tun:

- Die LAN IP-Adresse, die Subnetzmaske und den Domain-Suffix des CVE-30360 konfigurieren.
- Den internen DHCP-Server des CVE-30360 konfigurieren.
- Informationen über die im LAN an den CVE-30360 angeschlossenen Geräte abrufen.

Klicken Sie auf **LAN** > **LAN IP**. Die folgende Eingabemaske erscheint.

ABBILDUNG 10: Die Eingabemaske LAN > LAN IP



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 7: Die Eingabemaske LAN > LAN IP

WAN Informationen	
WAN IP Adresse	In diesem Feld wird die IP-Adresse des CVE-30360 an der WAN-Schnittstelle (Wide Area Network) angezeigt.
Subnet Mask	In diesem Feld wird die WAN-Subnetzmaske des CVE-30360 angezeigt.
Gateway-Adresse	In diesem Feld wird die Adresse des Geräts im WAN angezeigt, mit dem der CVE-30360 verbunden ist.
DNS Server	In diesem Feld werden die Domainnamen-Server angezeigt, die der CVE-30360 verwendet, um die Domainnamen in IP-Adressen umzuwandeln.
Private LAN IP Einstellungen	
Private LAN IP-Adresse	In diesem Feld können Sie die IP-Adressen des CVE-30360 im LAN festlegen.
Subnet Mask	In diesem Feld können Sie das LAN-Subnetz festlegen. Verwenden Sie die Dezimalschreibweise mit Trennpunkten (z. B. **255.255.255.0**).

TABELLE 7: Die Eingabemaske LAN > LAN IP (Fortsetzung)

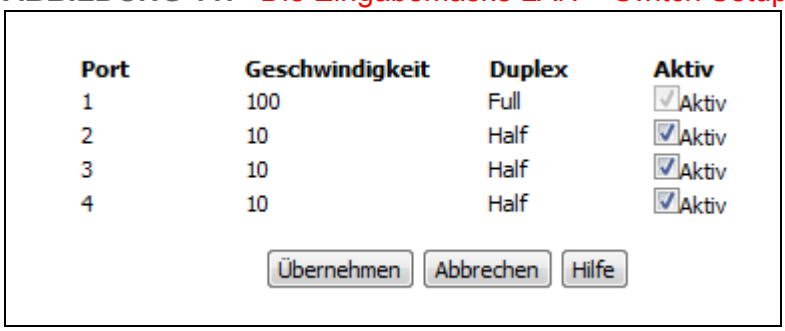
Domain-Suffix	In diesem Feld können Sie die Domain festlegen, die anstelle einer IP-Adresse in einen Webbrowser eingegeben werden kann, um im LAN auf den CVE-30360 zuzugreifen. *HINWEIS:* Der **Domain-Suffix** ist standardmäßig **hitronhub.home**.
Private LAN DHCP Einstellungen	
LAN DHCP	Wählen Sie diese Option, wenn der CVE-30360 den Netzwerkgeräten im LAN automatisch IP-Adressen zuweisen soll. Entfernen Sie die Markierung bei dieser Option, wenn bereits ein DHCP-Server im LAN vorhanden ist oder wenn Sie den Computern und anderen Netzwerkgeräten manuell IP-Adressen zuweisen möchten.
Lease Zeit	In diesem Feld können Sie festlegen, nach welcher Zeit der CVE-30360 die IP-Adressen aller im LAN an den CVE-30360 angeschlossenen Netzwerkgeräte erneuern soll (wenn DHCP aktiviert ist).
DHCP Start IP	In diesem Feld können Sie die erste IP-Adresse festlegen, die der CVE-30360 einem Gerät im LAN zuweist (wenn DHCP aktiviert ist).
DHCP End IP	In diesem Feld können Sie die letzte IP-Adresse festlegen, die der CVE-30360 einem Gerät im LAN zuweist (wenn DHCP aktiviert ist). *HINWEIS:* Geräte, die eine IP-Adresse anfordern, erhalten keine IP-Adresse mehr, wenn alle IP-Adressen aus dem DHCP-Pool verbraucht sind.
Host Name	Hier wird der Name aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
IP-Adresse	Hier wird die IP-Adresse aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
Typ	Hier wird angezeigt, ob die IP-Adresse des Geräts vom DHCP-Server (**DHCP-IP**) oder manuell **selbst vergeben** wurde.
Schnittstelle	Hier wird angezeigt, ob das Gerät über das LAN (**Ethernet**) oder das WLAN (**Wireless(x)** verbunden ist. Das **x** steht für den Drahtlosmodus **b**, **g** oder **n**).
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

3.3 DIE EINGABEMASKE SWITCH SETUP

Diese Maske enthält Informationen über die Datenrate und den Datenfluss aller **LAN**-Ports des CVE 30360. Hier können Sie einzelne Ports aktivieren oder deaktivieren.

Klicken Sie auf **LAN** > **Switch Setup**. Die folgende Eingabemaske erscheint.

ABBILDUNG 11: Die Eingabemaske LAN > Switch Setup



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 8: Die Eingabemaske LAN > Switch Setup

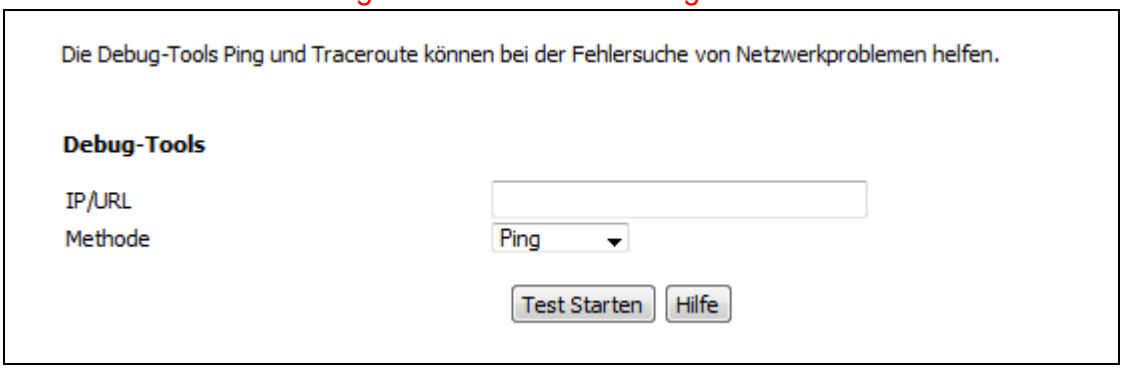
Port	Hier wird die LAN-Portnummer angezeigt.
Geschwindigkeit	Hier wird die maximal erreichbare Datengeschwindigkeit in Megabits pro Sekunde (MBPS) angezeigt.
Duplex	▶ Hier erscheint **full**, wenn die Daten zwischen dem CVE-30360 und dem angeschlossenen Gerät in beide Richtungen gleichzeitig fließen können. ▶ Hier erscheint **half**, wenn die Daten zwischen dem CVE-30360 und dem angeschlossenen Gerät in jeweils nur einer Richtung fließen können.
Aktiv	▶ Markieren Sie das Kontrollkästchen eines **Ports**, um die Kommunikation zwischen dem CVE-30360 und den an den Port angeschlossenen Geräten zu aktivieren. ▶ Entfernen Sie die Markierung aus dem Kontrollkästchen eines **Ports**, wenn keine Daten zwischen dem CVE-30360 und den an den Port angeschlossenen Geräten ausgetauscht werden sollen.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

3.4 DIE EINGABEMASKE DEBUG

Auf dieser Maske können Sie Pings und Traceroute-Tests für IP-Adressen oder URLs ausführen.

Klicken Sie auf **LAN** > **Debug**. Die folgende Eingabemaske erscheint.

ABBILDUNG 12: Die Eingabemaske LAN > Debug



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 9: Die Eingabemaske LAN > Fehlersuche

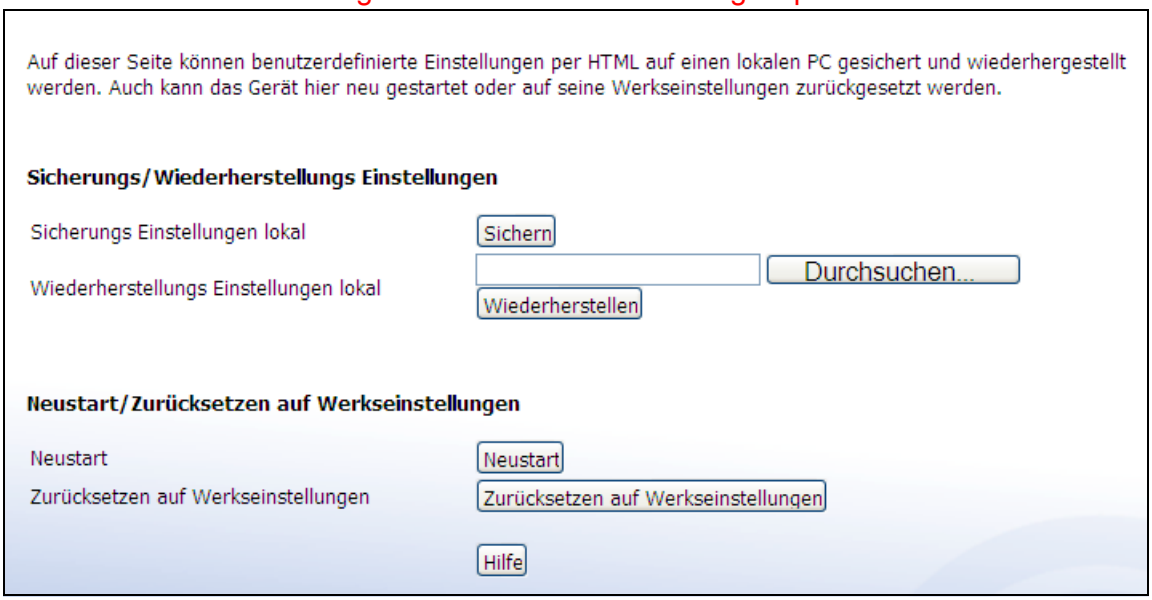
IP/URL	Geben Sie die IP-Adresse oder die URL ein, die Sie prüfen möchten.
Methode	Wählen Sie den Testtyp aus, den Sie auf die von Ihnen eingegebene **IP/URL** anwenden möchten.
Test Starten	Klicken Sie hier, um den Test auszuführen.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

3.5 DIE EINGABEMASKE SICHERUNGSKOPIE

Auf dieser Eingabemaske können Sie Ihre Einstellungen des CVE-30360 auf Ihrem Computer sichern, die Sicherung früherer Einstellungen laden, den CVE-30360 neu starten oder ihn auf seine Standardenstellungen zurücksetzen.

Klicken Sie auf **LAN** > **Sicherungskopie**. Die folgende Eingabemaske erscheint.

ABBILDUNG 13: Die Eingabemaske LAN > Sicherungskopie


Auf dieser Seite können benutzerdefinierte Einstellungen per HTML auf einen lokalen PC gesichert und wiederhergestellt werden. Auch kann das Gerät hier neu gestartet oder auf seine Werkseinstellungen zurückgesetzt werden.
Sicherungs/Wiederherstellungs Einstellungen
Sicherungs Einstellungen lokal
Sichern
Wiederherstellungs Einstellungen lokal
Durchsuchen...
Wiederherstellen
Neustart/Zurücksetzen auf Werkseinstellungen
Neustart
Neustart
Zurücksetzen auf Werkseinstellungen
Zurücksetzen auf Werkseinstellungen
Hilfe

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 10: Die Eingabemaske LAN > Sicherungskopie

Sicherungs/Wiederherstellungs Einstellungen	
Sicherungs Einstellungen lokal	Klicken Sie hier, um alle Einstellungen des CVE-30360 auf dem Computer zu sichern.
Wiederherstellungs Einstellungen lokal	Hier können Sie die Einstellungen des CVE-30360 entsprechend einer früheren Sicherung wieder herstellen. Klicken Sie auf **Durchsuchen**, um eine Sicherungsdatei auszuwählen, und dann auf **Wiederherstellen**, um die Einstellungen des CVE-30360 entsprechend denen der Sicherungsdatei zu konfigurieren.
Neustart/Zurücksetzen auf Werkseinstellungen	
Neustart	Klicken Sie hier, um den CVE-30360 zurückzusetzen.
Zurücksetzen auf Werkseinstellungen	Klicken Sie hier, um den CVE-30360 auf die Standardeinstellungen zurückzusetzen. ***HINWEIS:*** In diesem Fall gehen alle benutzerdefinierten Einstellungen verloren und können nicht wiederhergestellt werden.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4 FIREWALL

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **Firewall** klicken.

4.1 ÜBERSICHT ÜBER DEN MENÜPUNKT FIREWALL

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **Firewall** beschrieben.

4.1.1 FIREWALL

“Firewall” (Brandmauer) ist ursprünglich ein bautechnologischer Begriff. Er bezeichnet eine Mauer, die verhindern soll, dass sich ein Feuer auf andere Räume oder Gebäude ausbreitet. Ebenso verhindert die Firewall Ihres CVE-30360 Eindringversuche und andere unerwünschte Aktivitäten aus dem WAN, um die Computers Ihres LAN zu schützen. Sie können mit bestimmten Filtern festlegen, welche Computer und anderen Geräte auf das LAN zugreifen dürfen und welcher Datenverkehr vom LAN zum WAN verhindert werden soll.

4.1.2 PING

Mit dem CVE-30360 können Sie das Ping-Utility im LAN (bei **LAN** > **Fehlersuche**) und im WAN (bei **Firewall** > **Firewall-Optionen**) verwenden. Weitere Informationen dazu finden Sie unter Fehlersuche (Ping und Traceroute) auf Seite 34.

4.1.3 MAC-FILTER

Jedes Netzwerkgerät hat eine eindeutige MAC-Adresse, welche das Gerät im Netzwerk identifiziert. Wenn Sie den MAC-Adressfilter in der Firewall des CVE-30360 aktivieren, können Sie eine Liste von MAC-Adressen zusammenstellen und dann entscheiden, ob:

- den Geräten auf der Liste der Zugriff zum CVE-30360 und zum Netzwerk verwehrt werden soll (alle anderen Geräte können auf das Netzwerk zugreifen)

oder

- den Geräten auf der Liste der Zugriff auf das Netzwerk erlaubt werden soll (alle anderen Geräte können dann nicht auf das Netzwerk zugreifen).

4.1.4 IP-FILTERUNG

Mit dem IP-Filter können Sie verhindern, dass Computer des LAN bestimmte Datentypen in das WAN senden. Mit diesem Filter können Sie eine unerwünschte Kommunikation nach außen vermeiden. Legen Sie die IP-Adresse des Computers im LAN fest, von dem aus keine Kommunikation stattfinden soll. Legen Sie dann den Port-Bereich für die Kommunikation fest, die vermieden werden soll. Der CVE-30360 verwirft dann ausgehende Datenpakete, die den festgelegten Kriterien entsprechen.

4.1.5 PORT FORWARDING

Die Portweiterleitung ermöglicht es einem Computer im LAN, bestimmte Daten aus dem WAN zu empfangen. Das wird normalerweise verwendet, um bestimmte Anwendungen (z. B. Spiele) für einen bestimmten Computer im LAN durch die Firewall zuzulassen. Die Portweiterleitung wird auch häufig verwendet, um einen öffentlichen HTTP-Server von einem privaten Netzwerk aus laufen zu lassen.

Sie können für jede Anwendung, für die Sie Ports in der Firewall öffnen möchten, eine Portweiterleitungsregel festlegen. Wenn der CVE-30360 Daten aus dem WAN empfängt, deren Ziel ein Port ist, der einer Portweiterleitungsregel entspricht, werden die Daten zu der LAN IP-Adresse und Portnummer weitergeleitet, die in der Portweiterleitungsregel festgelegt wurden.

HINWEIS: Informationen dazu, welche Ports für eine bestimmte Anwendung geöffnet werden müssen, finden Sie in der Anleitung zur jeweiligen Anwendung.

HINWEIS: Diese Funktion ist nicht verfügbar, wenn DS-lite aktiviert ist.

4.1.6 PORT TRIGGERING

Port-Triggering ist ein Mittel der automatischen Portweiterleitung. Der CVE-30360 prüft den ausgehenden Datenverkehr (vom LAN zum WAN), um festzustellen, ob Sie für die angegebenen Zielports Port-Triggering-Regeln festgelegt haben. Wenn es Übereinstimmungen gibt, öffnet der CVE-30360 in Erwartung von eingehendem Verkehr automatisch die in der Regel festgelegten Eingangsports.

HINWEIS: Diese Funktion ist nicht verfügbar, wenn DS-lite aktiviert ist.

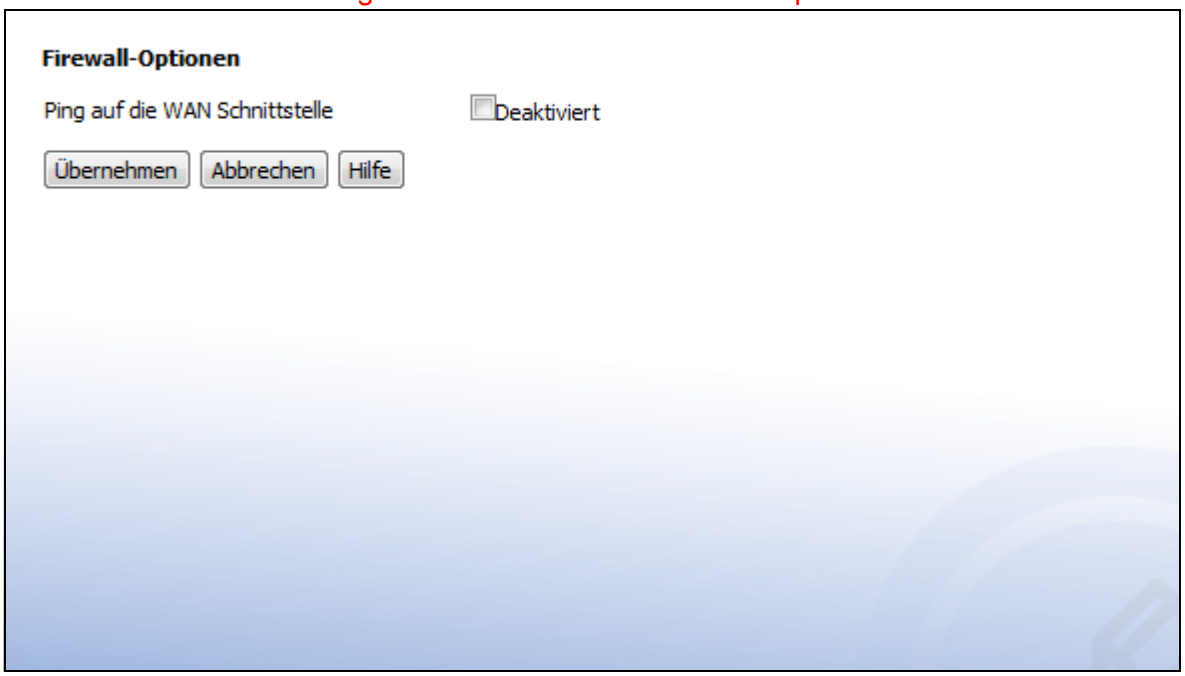
4.2 DIE EINGABEMASKE FIREWALL-OPTIONEN

In dieser Maske können Sie die Firewall-Funktionen ein- oder ausschalten und die DMZ Ihres Netzwerks konfigurieren. Sie können das Intrusion-Detection-System des CVE-30360 aktivieren oder deaktivieren und Reaktionen auf ICMP-Anfragen aus dem WAN zulassen oder verhindern.

HINWEIS: Es kann sich jeweils immer nur ein Gerät in der DMZ befinden.

Klicken Sie auf **Firewall** > **Firewall-Optionen**. Die folgende Eingabemaske erscheint.

ABBILDUNG 14: Die Eingabemaske Firewall > Firewall-Optionen



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 11: Die Eingabemaske Firewall > Firewall-Optionen

Intrusion Detection System	▲ Mit dieser Option können Sie das Intrusion-Detection-System ausschalten. ▲ Mit dieser Option können Sie das Intrusion-Detection-System einschalten.
Ping auf die WAN Schnittstelle	▲ Mit dieser Option können Sie Reaktionen auf ICMP-Anfragen aus dem WAN verhindern. ▲ Mit dieser Option können Sie Reaktionen auf ICMP-Anfragen aus dem WAN zulassen.
DMZ Host Aktivieren	In diesem Feld können Sie die DMZ ein- oder ausschalten. ▲ Markieren Sie das Kontrollkästchen, um die DMZ zu aktivieren. ▲ Entfernen Sie die Markierung aus dem Kontrollkästchen, um die DMZ zu deaktivieren. Computer, die sich zuvor in der DMZ befanden, befinden sich nun im LAN.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
[...] IP-Adresse [...]	Geben Sie die IP-Adresse des Computers ein, den Sie zur DMZ unten hinzufügen möchten.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.3 DIE EINGABEMASKE MAC-FILTER

In diesem Fenster konfigurieren Sie die MAC-Adressfilterfunktion im LAN.

HINWEIS: Eine Beschreibung, wie der MAC-Adressfilter im WLAN konfiguriert wird, finden Sie unter DIE EINGABEMASKE ZUGANGS KONTROLLE auf Seite 70.

Sie können den CVE-30360 so einstellen, dass er nur bestimmten Geräten den Zugriff zum CVE-30360 und zum Netzwerk gewährt, ihn aber anderen Geräten verweigert.

HINWEIS: Eine Liste aller Computer, die im LAN mit dem CVE-30360 verbunden sind, können Sie aufrufen, indem Sie bei **Firewall** > **IP-Filterung**, **Port Forwarding**, **Port Triggering** oder **Firewall-Optionen** auf die Schaltfläche **Angeschlossene Computer** klicken.

Klicken Sie auf **Firewall** > **MAC-Filter**. Die folgende Eingabemaske erscheint.

ABBILDUNG 15: Die Eingabemaske Firewall > MAC-Filter

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 12: Die Eingabemaske Firewall > MAC-Filter

MAC-Filter-Optionen	
MAC-Filter-Optionen	Hier können Sie festlegen, ob der CVE-30360 einen MAC-Filter anwenden soll. ▸ Wählen Sie **Alle erlauben**, um den MAC-Filter auszuschalten. Alle Geräte können auf den CVE-30360 und auf das Netzwerk zugreifen. ▸ Wählen Sie **Erlauben**, damit nur Geräte, deren MAC-Adresse sich in der **Tabelle zugelassene Geräte** befinden, auf den CVE-30360 und das Netzwerk zugreifen können. Allen anderen Geräten wird der Zugriff verwehrt. ▸ Wenn Sie **Verbieten** wählen, erhalten alle Geräte den Zugriff auf den CVE-30360 und auf das Netzwerk. Ausgenommen sind die Geräte, deren MAC-Adresse in der **Tabelle verweigerte Geräte** stehen. Den angegebenen Geräten wird der Zugriff verweigert.
Tabelle zugelassene Geräte (bis zu 16 Einträge)	
#	Hier wird die Indexnummer der zugelassenen Geräte angezeigt.
Geräte Name	Hier wird der Name des zugelassenen Geräts angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse des zugelassenen Geräts angezeigt.
Löschen	Klicken Sie auf die Optionsschaltfläche eines zugelassenen Geräts ( ), um das Gerät aus der Liste zu entfernen. Das Gerät hat dann keinen Zugriff mehr auf den CVE-30360 und auf das Netzwerk. ***HINWEIS:*** Löschen Sie auf keinen Fall Ihren Verwaltungscomputer aus der Liste. Sollte das doch einmal passieren, müssen Sie sich von einem anderen Computer aus wieder anmelden oder den CVE-30360 zurücksetzen.
Tabelle verweigerte Geräte (bis zu 16 Einträge)	
Gerätename	Hier wird der Name des nicht zugelassenen Geräts angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse des nicht zugelassenen Geräts angezeigt.
Löschen	Klicken Sie auf die Optionsschaltfläche eines abgelehnten Geräts ( ), um das Gerät aus der Liste zu entfernen. Das Gerät hat dann wieder Zugriff mehr auf den CVE-30360 und auf das Netzwerk.

TABELLE 12: Die Eingabemaske Firewall > MAC-Filter (Fortsetzung)

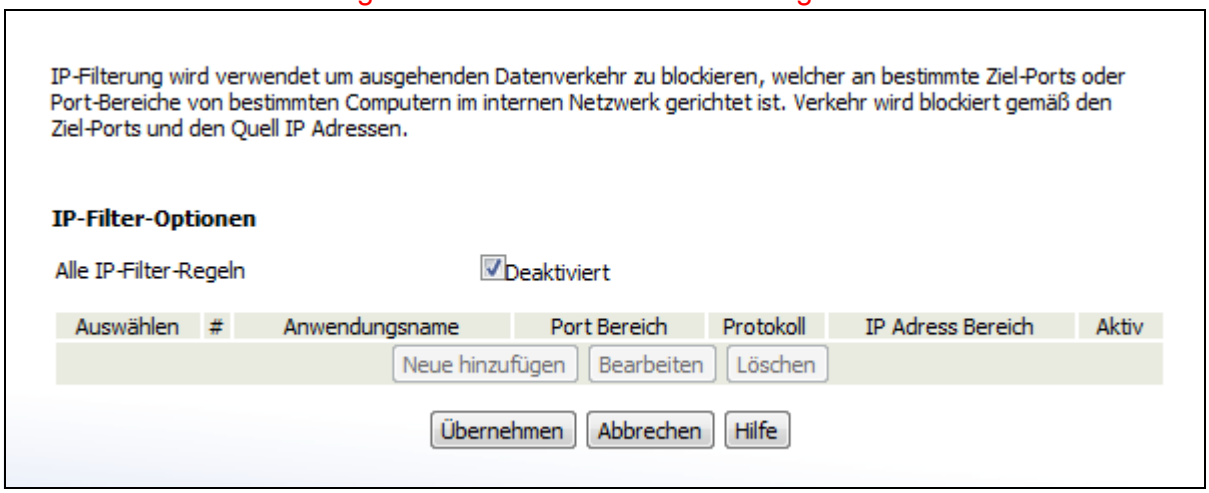
Automatisch erlernte LAN-Geräte	
Geräte Name	Hier wird der Name aller Netzwerkgeräte angezeigt, die im LAN mit dem CVE-30360 verbunden sind.
MAC-Adresse	Hier wird die MAC-Adresse aller Netzwerkgeräte angezeigt, die im LAN mit dem CVE-30360 verbunden sind.
Typ	In diesem Feld können Sie die Liste auswählen, zu der Sie das Gerät hinzufügen möchten. ▶ Wählen Sie **Erlauben**, um das Gerät zur **Tabelle zugelassene Geräte** hinzuzufügen. ▶ Wählen Sie **Verbieten**, um das Gerät zur **Tabelle verweigerte Geräte** hinzuzufügen.
Manuell hinzugefügte LAN-Geräte	
Geräte Name	Geben Sie den Namen des Netzwerkgeräts ein, dem der Zugriff zum CVE-30360 und zum Netzwerk gewährt oder verweigert werden soll. *HINWEIS:* Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
MAC-Adresse	Geben Sie die MAC-Adresse des Netzwerkgeräts ein, für das Sie den Zugriff auf den CVE-30360 und das Netzwerk zulassen oder verweigern möchten.
Typ	In diesem Feld können Sie die Liste auswählen, zu der Sie das Gerät hinzufügen möchten. ▶ Wählen Sie **Erlauben**, um das Gerät zur **Tabelle zugelassene Geräte** hinzuzufügen. ▶ Wählen Sie **Verbieten**, um das Gerät zur **Tabelle verweigerte Geräte** hinzuzufügen.
Hinzufügen	Klicken Sie hier, um das Gerät zu der von Ihnen festgelegten Liste hinzuzufügen.
Abbrechen	Klicken Sie hier, um die Felder **Manuell hinzugefügte LAN-Geräte** zu löschen.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.4 DIE EINGABEMASKE IP-FILTERUNG

Auf dieser Eingabemaske konfigurieren Sie den IP-Filter. Sie können den IP-Filter aktivieren oder deaktivieren und bestehende IP-Filterregeln ändern und neue konfigurieren.

Klicken Sie auf **Firewall** > **IP-Filter**. Die folgende Eingabemaske erscheint.

ABBILDUNG 16: Die Eingabemaske Firewall > IP-Filterung



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 13: Die Eingabemaske Firewall > IP-Filterung

Alle IP-Filter-Regeln	Hier können Sie den IP-Filter ein- oder ausschalten. ▶ Entfernen Sie die Markierung aus dem Kontrollkästchen, um den IP-Filter zu aktivieren. ▶ Markieren Sie das Kontrollkästchen, um den IP-Filter zu deaktivieren (Standardeinstellung). *HINWEIS:* Sie können IP-Filterregeln nur dann hinzufügen, bearbeiten oder löschen, wenn dieses Kontrollkästchen nicht markiert ist.
Auswählen	Wählen Sie die Optionsschaltfläche einer IP-Filterregel (◉), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der IP-Filterregel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port Bereich	Hier werden der Start- und Endport des Bereichs angezeigt, dem die Kommunikation mit den festgelegten IP-Adressen untersagt ist.
Protokoll	Hier werden die nicht zugelassenen Kommunikationstypen angezeigt: ▶ **TCP** - die Kommunikation mit dem Transmission Control Protocol ist nicht zugelassen. ▶ **UDP** - die Kommunikation mit dem User Datagram Protocol ist nicht zugelassen. ▶ **TCP/UDP** - die Kommunikation mit dem Transmission Control Protocol und dem User Datagram Protocol ist nicht zugelassen.
IP Adress Bereich	Hier wird die erste und letzte IP-Adresse des Bereichs angezeigt, dem die Kommunikation mit den festgelegten Ports untersagt wird.

TABELLE 13: Die Eingabemaske Firewall > IP-Filterung (Fortsetzung)

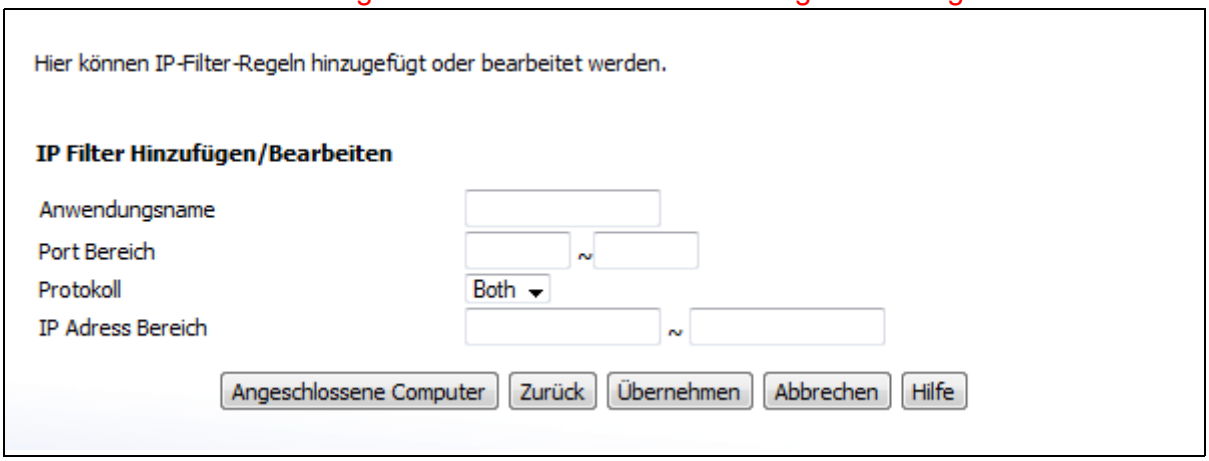
AKtiv	Hier können Sie jede IP-Filterregel ein- oder ausschalten. ▶ Markieren Sie dieses Kontrollkästchen, um die IP-Filterregel zu aktivieren. ▶ Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die IP-Filterregel zu deaktivieren.
Hinzufügen	Klicken Sie hier, um eine neue IP-Filterregel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IP-Filterregel auf Seite 48.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der IP-Filterregel (), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IP-Filterregel auf Seite 48.
Löschen	Klicken Sie die auf die Optionsschaltfläche der IP-Filterregel (), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.4.1 HINZUFÜGEN ODER BEARBEITEN EINER IP-FILTERREGEL

- Um eine neue IP-Filterregel hinzuzufügen, klicken Sie in der Eingabemaske **Firewall** > **IP-Filterung** auf **Neue hinzufügen**.
- Um eine vorhandene IP-Filterregel zu bearbeiten, wählen Sie die Optionsschaltfläche () auf der Eingabemaske **Firewall** > **IP-Filterung**, und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

ABBILDUNG 17: Die Eingabemaske Firewall > IP-Filterung > Hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 14: Die Eingabemaske Firewall > IP-filterung > Hinzufügen/Bearbeiten

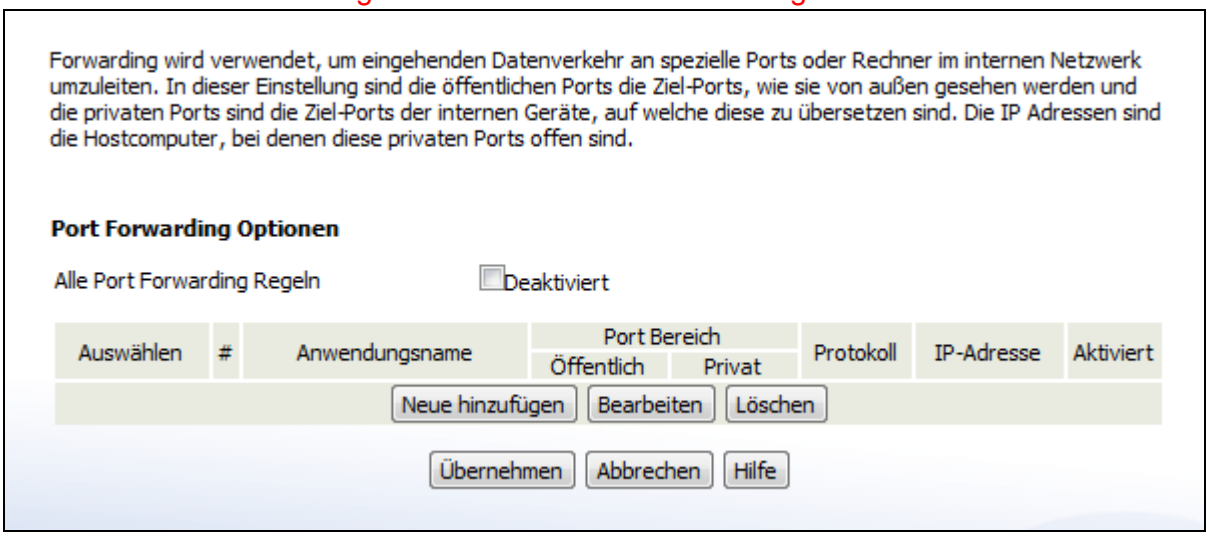
Anwendungsname	Geben Sie den Namen für die Anwendung ein, die Sie sperren möchten. ***HINWEIS:*** Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Port Bereich	Hier können Sie den Zielportbereich festlegen für den die Kommunikation gesperrt ist. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Protokoll	Hier können Sie festlegen, ob der CVE-30360 eine der folgenden Kommunikationstypen sperren soll: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ **Both** - TCP und UDP ***HINWEIS:*** Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**Both**) beibehalten.
IP Adress Bereich	In diesen Feldern können Sie den IP-Adressbereich der lokalen Computer festlegen deren Kommunikation gesperrt werden soll. Geben Sie die erste IP-Adresse in das erste Feld und die letzte IP-Adresse in das zweite Feld ein. Wenn Sie nur eine einzelne IP-Adresse festlegen möchten, geben Sie in beide Felder dieselbe Adresse ein.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Firewall** > **IP-Filterung** zurückzukehren, ohne die Änderungen in der IP-Filterregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.5 DIE EINGABEMASKE FORWARDING

Auf dieser Eingabemaske konfigurieren Sie die Portweiterleitung zwischen den Computern im WAN und den Computern im the LAN. Sie können die Portweiterleitung aktivieren oder deaktivieren, vorhandene Portweiterleitungsregeln ändern und neue konfigurieren.

Klicken Sie auf **Firewall** > **Forwarding**. Die folgende Eingabemaske erscheint.

ABBILDUNG 18: Die Eingabemaske Firewall > Forwarding


Forwarding wird verwendet, um eingehenden Datenverkehr an spezielle Ports oder Rechner im internen Netzwerk umzuleiten. In dieser Einstellung sind die öffentlichen Ports die Ziel-Ports, wie sie von außen gesehen werden und die privaten Ports sind die Ziel-Ports der internen Geräte, auf welche diese zu übersetzen sind. Die IP Adressen sind die Hostcomputer, bei denen diese privaten Ports offen sind.
Port Forwarding Optionen
Alle Port Forwarding Regeln
Deaktiviert
Auswählen
#
Anwendungsname
Port Bereich
Öffentlich
Privat
Protokoll
IP-Adresse
Aktiviert
Neue hinzufügen
Bearbeiten
Löschen
Übernehmen
Abbrechen
Hilfe

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 15: Die Eingabemaske Firewall > Forwarding

Alle Port Forwarding Regeln	In diesem Feld können Sie die Portweiterleitung ein- oder ausschalten. ▶ Markieren Sie das Kontrollkästchen, um die Portweiterleitung zu aktivieren. ▶ Entfernen Sie die Markierung aus dem Kontrollkästchen, um die Portweiterleitung zu deaktivieren.
Auswählen	Wählen Sie die Optionsschaltfläche einer Portweiterleitungsregel ( ), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der Portweiterleitungsregel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port Bereich	In diesen Feldern werden die Ports angezeigt, für die die Regel gilt: ▶ Im Feld **Öffentlich** wird der eingehende Portbereich angezeigt. Das sind die Ports, auf denen der CVE-30360 Daten vom Host im WAN erhalten hat. ▶ Im Feld **Privat** wird der Portbereich angezeigt, zu dem der CVE-30360 Daten, die an das Gerät im LAN adressiert sind, weiterleitet.
Protokoll	In diesem Feld wird das/werden die Protokoll(e) angezeigt, für die diese Regel gilt: ▶ Transmission Control Protocol (**TCP**) ▶ User Datagram Protocol (**UDP**) ▶ Transmission Control Protocol und User Datagram Protocol (**TCP/UDP**) ▶ Generic Routing Encapsulation (**GRE**) ▶ Encapsulating Security Protocol (**ESP**)

TABELLE 15: Die Eingabemaske Firewall > Forwarding (Fortsetzung)

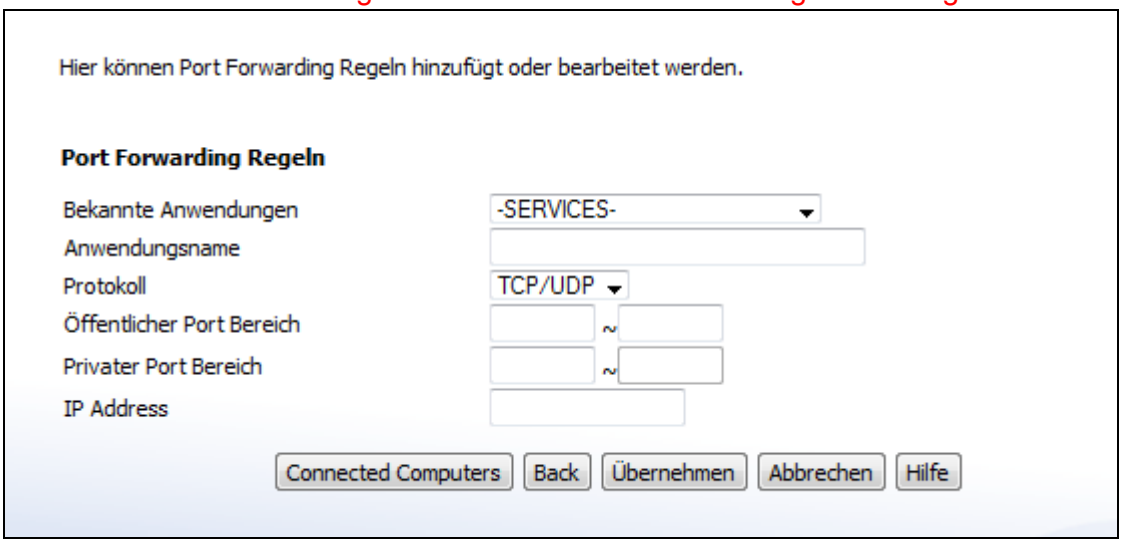
IP-Adresse	Hier wird die IP-Adresse des Computers im LAN angezeigt, zu dem der Datenverkehr weitergeleitet wird, der den Bedingungen **Öffentlicher Portbereich** und **Protokoll** entspricht.
Aktiviert	Hier können Sie jede Portweiterleitungsregel ein- oder ausschalten. ▶ Markieren Sie dieses Kontrollkästchen, um die Portweiterleitungsregel zu aktivieren. ▶ Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die Portweiterleitungsregel zu deaktivieren.
Hinzufügen	Klicken Sie hier, um eine neue Portweiterleitungsregel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Portweiterleitungsregel auf Seite 51.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der Portweiterleitungsregel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Portweiterleitungsregel auf Seite 51.
Löschen	Klicken Sie die auf die Optionsschaltfläche der Portweiterleitungsregel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.5.1 HINZUFÜGEN ODER BEARBEITEN EINER PORTWEITERLEITUNGSREGEL

- Um eine neue Portweiterleitungsregel hinzuzufügen, klicken Sie in der Eingabemaske **Firewall** > **Forwarding** auf **Neue hinzufügen**.
- Um eine vorhandene Portweiterleitungsregel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Firewall** > **Forwarding**, und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

ABBILDUNG 19: Die Eingabemaske Firewall > Forwarding > Hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 16: Die Eingabemaske Firewall > Forwarding > Hinzufügen/Bearbeiten

Anwendungsname	Geben Sie einen Namen für die Anwendung ein, für die Sie eine neue Regel festlegen möchten. *HINWEIS:* Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Öffentlicher Port Bereich	In diesen Feldern können Sie den eingehenden Portbereich festlegen. Das sind die Ports, auf denen der CVE-30360 Daten vom Host im WAN erhalten hat. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Privater Port Bereich	In diesen Feldern können Sie die Ports festlegen, an die der empfangene Datenverkehr weitergeleitet werden soll. Geben Sie die erste Portnummer in das erste Feld ein. Die Anzahl der Ports muss mit der unter **Öffentlicher Port Bereich** festgelegten Anzahl übereinstimmen. Der CVE-30360 ergänzt dann automatisch das zweite Feld.
Protokoll	Hier können Sie festlegen, ob der CVE-30360 eine der folgenden Kommunikationstypen weiterleiten soll: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol und User Datagram Protocol (**TCP/UDP**) ▸ Generic Routing Encapsulation (**GRE**) ▸ Encapsulating Security Protocol (**ESP**) *HINWEIS:* Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**TCP/UDP**) beibehalten.
IP-Adresse	In dieses Feld können Sie die IP-Adresse des Computers im LAN eingeben, zu dem der Datenverkehr weitergeleitet werden soll.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.

TABELLE 16: Die Eingabemaske Firewall > Forwarding > Hinzufügen/Bearbeiten

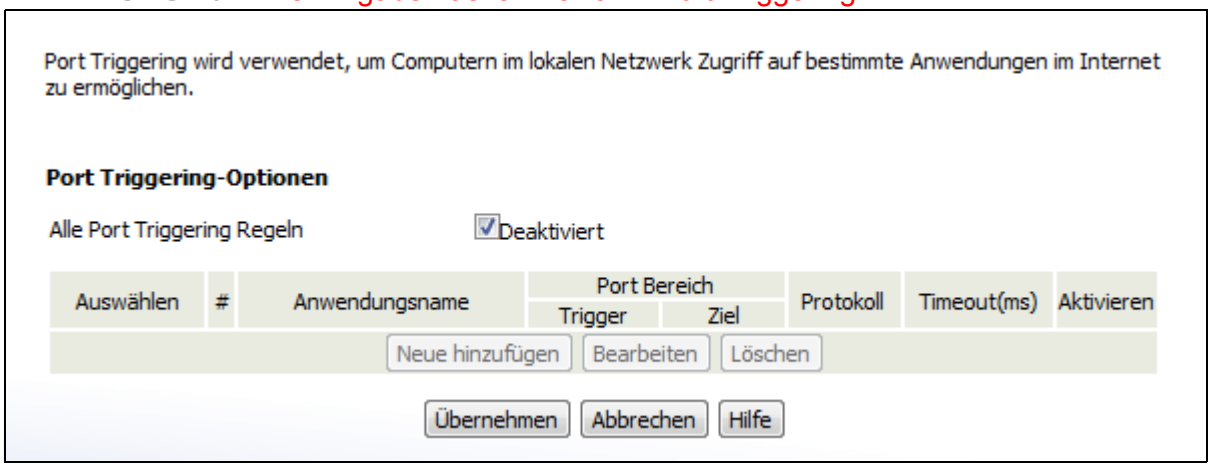
Zurück	Klicken Sie hier, um zur Eingabemaske **Firewall** > **Forwarding** zurückzukehren, ohne die Änderungen in der Portweiterleitungsregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.6 DIE EINGABEMASKE PORT TRIGGERING

Auf dieser Eingabemaske konfigurieren Sie das Port-Triggering. Sie können das Port-Triggering aktivieren oder deaktivieren, vorhandene Port-Triggering-Regeln ändern und neue konfigurieren.

Klicken Sie auf **Firewall** > **Port Triggering**. Die folgende Eingabemaske erscheint.

ABBILDUNG 20: Die Eingabemaske Firewall > Port Triggering



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 17: Die Eingabemaske Firewall > Port Triggering

Alle Port Triggering Regeln	In diesem Feld können Sie das Port-Triggering ein- oder ausschalten. ▶ Markieren Sie das Kontrollkästchen, um das Port-Triggering zu aktivieren. ▶ Entfernen Sie die Markierung aus dem Kontrollkästchen, um das Port-Triggering zu deaktivieren.
Auswählen	Wählen Sie die Optionsschaltfläche einer Port-Triggering-Regel ( ), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der Port-Triggering-Regel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.

TABELLE 17: Die Eingabemaske Firewall > Port Triggering

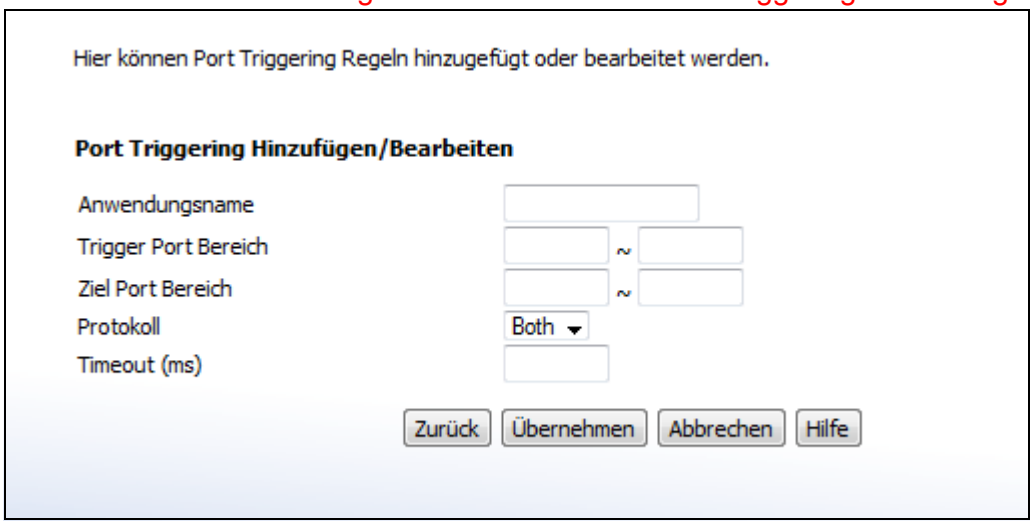
Port Bereich	In diesen Feldern werden die Ports angezeigt, für die die Regel gilt: • Im Feld **Trigger** wird der Bereich der ausgehenden Ports angezeigt. Wenn der CVE-30360 an diesen Ports von den Computern des LAN ausgehenden Datenverkehr erkennt, öffnet er automatisch die **Ziel**-Ports. • Im Feld **Ziel** wird der Bereich der getriggerten Ports angezeigt. Diese Ports werden automatisch geöffnet, wenn der CVE-30360 Aktivitäten von den Computern des LAN an den **Trigger**-Ports erkennt.
Protokoll	Hier wird das Protokoll der Port-Triggering-Regel angezeigt.
Timeout (ms)	Nachdem der CVE-30360 die **Ziel**-Ports geöffnet hat, wird hier die Zeit (in Millisekunden) angezeigt, nach der die Ports wieder geschlossen werden müssen.
Aktivieren	Hier können Sie jede Port-Triggering-Regel ein- oder ausschalten. • Markieren Sie dieses Kontrollkästchen, um die Port-Triggering-Regel zu aktivieren. • Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die Port-Triggering-Regel zu deaktivieren.
Hinzufügen	Klicken Sie hier, um eine neue Port-Triggering-Regel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Port-Triggering-Regel auf Seite 54.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der Port-Triggering-Regel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Port-Triggering-Regel auf Seite 54.
Löschen	Klicken Sie die auf die Optionsschaltfläche der Port-Triggering-Regel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

4.6.1 HINZUFÜGEN ODER BEARBEITEN EINER PORT-TRIGGERING-REGEL

- Um eine neue Port-Triggering-Regel hinzuzufügen, klicken Sie in der Eingabemaske **Firewall** > **Port Triggering** auf **Neue hinzufügen**.
- Um eine vorhandene Port-Triggering-Regel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Firewall** > **Port Triggering**, und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

ABBILDUNG 21: Die Eingabemaske Firewall > Port Triggering > Hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 18: Die Eingabemaske Firewall > Port Triggering > Hinzufügen/Bearbeiten

Anwendungsname	Geben Sie einen Namen für die Anwendung ein, für die Sie eine neue Regel festlegen möchten. *HINWEIS:* Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Trigger Port Bereich	In diesen Feldern können Sie die Trigger-Ports festlegen. Wenn der CVE-30360 an einem dieser Ports Aktivitäten von einem Computer des LAN erkennt, öffnet er in Erwartung eingehender Daten automatisch die **Ziel**-Ports. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Ziel Port Bereich	In diesen Feldern können Sie die Ziel-Ports festlegen. Der CVE-30360 öffnet diese Ports in Erwartung eingehender Daten, sobald er Aktivitäten an einem der **Trigger**-Ports ermittelt. Der eingehende Datenverkehr wird an diese Ports des mit dem LAN verbundenen Computers weitergeleitet. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Protokoll	In diesem Feld können Sie festlegen, ob der CVE-30360 diesen Trigger aktivieren soll, wenn er Aktivitäten mit den folgenden Protokollen erkennt: - Transmission Control Protocol (**TCP**) - User Datagram Protocol (**UDP**) - Transmission Control Protocol und User Datagram Protocol (**Both**) *HINWEIS:* Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**Beide**) beibehalten.
Timeout (ms)	Geben Sie hier die Zeit (in Millisekunden) ein, nachdem der CVE-30360 die **Ziel**-Ports geöffnet hat, nach der die Ports wieder geschlossen werden sollen.

TABELLE 18: Die Eingabemaske Firewall > Port Triggering > Hinzufügen/Bearbeiten

Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Firewall** > **Forwarding** zurückzukehren, ohne die Änderungen in der Portweiterleitungsregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

5 WIRELESS

In diesem Kapitel erhalten Sie eine kurze Einführung in den Umgang mit Drahtlosnetzwerken. Im Folgenden werden einige grundsätzliche Schritte zum Einrichten eines Netzwerks beschrieben, und Sie erhalten einen Überblick über die Einstellungsmöglichkeiten des Menüpunkts **Wireless**, welcher aus den folgenden Abschnitten besteht:

- Grundeinstellungen des Drahtlosnetzwerks auf Seite 57: Hier erfahren Sie, wie Drahtlosnetzwerke funktionieren und wie sie gesichert werden können.
- Anleitung zur Nutzung der Drahtlosfunktion auf Seite 59: Hier erfahren Sie, wie Sie mit dem CVE-30360 einige Grundeinstellungen für das Drahtlosnetzwerk konfigurieren können.
- Erweiterte Drahtlosnetzwerkfunktionen auf Seite 62: Hier erhalten Sie einige weiterführende Informationen zu diesem Thema.
  Wenn Sie das Drahtlosnetzwerk nur in einer Standardkonfiguration einrichten möchten, müssen Sie diesen Abschnitt nicht lesen.
- Die Eingabemasken für die Drahtloskonfiguration auf Seite 64: Hier erhalten Sie eine ausführliche Beschreibung der Eingabemasken für die Drahtloskonfiguration des CVE-30360.
  Anhand dieser Beschreibung können Sie Informationen zu bestimmten Eingabemasken oder Feldern leichter finden.

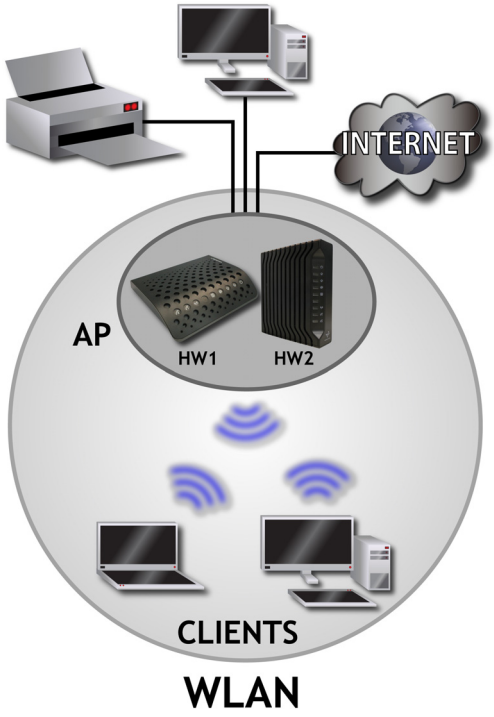
5.1 GRUNDEINSTELLUNGEN DES DRAHTLOSNETZWERKS

In diesem Abschnitt wird beschrieben, wie Drahtlosnetzwerke und ihre Sicherheitsfunktionen funktionieren.

Das Drahtlosnetzwerk (Wireless LAN oder WLAN) des CVE-30360 ist der kabellose Teil eines Local Area Network (LAN). Das WLAN ist ein Netzwerk von Funkverbindungen zwischen dem CVE-30360 und den daran angeschlossenen Computern und Geräten.

In der folgenden Abbildung ist das Drahtlosnetzwerk durch den Kreis gekennzeichnet. Das Notebook und der PC sind die Wireless Clients, die an den CVE-30360, dem Zugriffspunkt oder auch Access Point (AP) angeschlossen sind. Die Wireless Clients nutzen den AP, um auf andere Geräte (z. B. den Drucker) oder auf das Internet zuzugreifen.

ABBILDUNG 22: Beispiel für ein Drahtlosnetzwerk



5.1.1 WLAN-STANDARDS

Wie Drahtlosgeräte miteinander kommunizieren, wird vom Institute of Electrical and Electronics Engineers (IEEE) standardisiert. Die IEEE-Standards für Wireless LANs sind an ihrer Bezeichnung 802.11 zu erkennen. Es gibt verschiedene WLAN-Standards, von denen der CVE-30360 nur die Folgenden unterstützt (sortiert nach Einführung - von alt nach neu - und Datenübertragungsgeschwindigkeit - niedrig nach hoch):

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

5.1.2 SERVICE SETS UND SSIDS

Alle Geräte eines Drahtlosnetzwerks bilden zusammen das sogenannte Service Set.

Jedes Service Set ist durch einen Service Set IDentifier (SSID) gekennzeichnet. Dieses ist der Name des Netzwerks. Den Wireless Clients muss die SSID bekannt sein, damit sie die Verbindung zum AP herstellen können.

Sie können den CVE-30360 so konfigurieren, dass er die SSID sendet (in diesem Fall kann jeder Client, der die Funkwellen abtastet, die SSID erkennen) oder die SSID verbirgt (in diesem Fall wird sie nicht ausgesendet, sodass nur die Benutzer, welche die SSID kennen, eine Verbindung herstellen können). Weitere Informationen dazu finden Sie unter Verbergen des Netzwerks auf Seite 61.

5.1.3 GRUNDLAGEN FÜR DIE WLAN-SICHERHEIT

Die Funkübertragung ist an sich ein unsicheres Medium, da sie innerhalb der Reichweite von jedem empfangen werden kann, der über ein Empfangsgerät verfügt. Aus diesem Grund gibt es unterschiedliche Verfahren, diese Art der Übertragung sicherer zu machen.

Diese Verfahren steuern die Authentifizierung (es wird festgelegt, wer Zugriff zum Netzwerk haben soll) und die Verschlüsselung (verschlüsselte Signale können nur von authentifizierten Benutzern entschlüsselt werden). Die Ausgereiftheit sowie die Effektivität jeder dieser Sicherheitsverfahren sind sehr unterschiedlich.

Der CVE-30360 unterstützt die folgenden drahtlosen Sicherheitsprotokolle (angeordnet nach Effektivität):

- geringste Sicherheit
- keine Sicherheit
- WEP
- WPA-PSK
- WPA2-PSK
- größte Sicherheit

Weitere Informationen zu diesen Sicherheitsprotokollen finden Sie unter Erweiterte Sicherheitseinstellungen im Drahtlosnetzwerk auf Seite 62.

5.2 ANLEITUNG ZUR NUTZUNG DER DRAHTLOSFUNKTION

In diesem Abschnitt werden grundlegende Netzwerkverwaltungsaufgaben beschrieben.

HINWEIS: Eine Beschreibung der Grundlagen zum Einrichten des Drahtlosnetzwerks finden Sie in der Kurzanleitung, die Sie zusammen mit dem CVE-30360 erhalten haben.

Dazu gehören:

- Auswählen eines Sicherheitsverfahrens auf Seite 59
- Wechseln des Passworts für den Zugriff auf das Drahtlosnetzwerk auf Seite 60
- Ändern des Netzwerknamens (SSID) auf Seite 61
- Verbergen des Netzwerks auf Seite 61
- Verbessern der Leistung des Drahtlosnetzwerks auf Seite 61

5.2.1 AUSWÄHLEN EINES SICHERHEITSVERFAHRENS

Welches Sicherheitsverfahren Sie für Ihr Drahtlosnetzwerk auswählen, ist abhängig von den Sicherheitsverfahren, die Ihre Geräte im Netzwerk (der CVE-30360, Ihr PC, Ihr Notebook usw.) unterstützen.

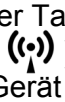
Nicht alle Geräte unterstützen alle Verfahren. Sie müssen also zuerst herausfinden, welche Verfahren die Geräte unterstützen und dann ein Verfahren auswählen, welches von allen Geräten unterstützt wird.

Ziel ist es immer, das bestmögliche Sicherheitsverfahren auszuwählen. Eine Liste der Verfahren, die der CVE-30360 unterstützt, finden Sie unter Grundlagen für die WLAN-Sicherheit auf Seite 59 (sortiert nach Effizienz).

So können Sie herausfinden, welche Sicherheitsverfahren die anderen Drahtlosgeräte unterstützen:

- Möglicherweise befindet sich am Gerät ein Etikett, auf dem die unterstützten Verfahren aufgeführt sind.
- Informationen zu den unterstützten Sicherheitsverfahren können in der Dokumentation oder auf der Verpackung des jeweiligen Geräts enthalten sein.
- Im Konfigurationsprogramm des Geräts finden Sie eine Liste der unterstützten Verfahren. Es handelt sich meist um eine Dropdown-Liste, aus der Sie eine Option auswählen können.
- Auf der Website des Geräteherstellers gibt es möglicherweise eine Seite, auf der die Spezifikationen des Geräts aufgeführt sind.

Wenn Sie WPS (siehe WPS auf Seite 63) verwenden möchten, müssen alle Wireless Clients WPS unterstützen. Neben den oben beschriebenen Möglichkeiten gibt es zwei weitere Möglichkeiten herauszufinden, ob das der Fall ist:

- Suchen Sie auf dem Drahtlosgerät nach einer Taste, die mit “WPS” oder ähnlich bezeichnet ist oder ein Wellensymbol (z. B. ) oder das “Wi-Fi Protected Setup”-Logo trägt. Ist das der Fall, unterstützt das Gerät wahrscheinlich das WPS-PBC-Verfahren (“Push-Button Configuration”).
- Rufen Sie das Konfigurationsprogramm des Drahtlosgeräts auf, und suchen Sie nach einem Menüpunkt mit der Bezeichnung “WPS” oder “Wi-Fi Protected Setup”. Hier sollte zu erkennen sein, ob das Gerät das WPS-PBC-Verfahren, das WPS-PIN-Verfahren oder sogar beide Verfahren unterstützt (einige Geräte verfügen zusätzlich zu oder anstelle einer physischen Taste am Gerät auch über eine PBC-Taste in ihrem Konfigurationsprogramm).

Wenn Sie sich für ein Sicherheitsverfahren entschieden haben, können Sie dieses am CVE-30360 im Menüpunkt **Wireless** > **Sicherheit** bei **Sicherheits Modus** (siehe Die Eingabemaske Sicherheit auf Seite 66) einstellen.

5.2.2 WECHSELN DES PASSWORTS FÜR DEN ZUGRIFF AUF DAS DRAHTLOSNETZWERK

Nur Wireless Clients mit dem richtigen Passwort können auf das Netzwerk zugreifen. Es wird empfohlen, das Passwort des Drahtlosnetzwerks häufiger zu wechseln, vor allem dann, wenn Sie wissen, dass Unbefugte ihr Passwort kennen oder verdächtige Aktivitäten im Netzwerk auftreten.

Das Passwort muss zunächst am CVE-30360 und dann an allen Wireless Clients geändert werden.

Das Verfahren zum Ändern des Passworts am CVE-30360 ist abhängig vom verwendeten Sicherheitsverfahren.

- Wenn Sie das Sicherheitsverfahren WPS-PBC verwenden, bei dem Sie eine Taste am CVE-30360 und dann an den Drahtlosgeräten drücken müssen, damit sich die Geräte automatisch verbinden, müssen Sie lediglich das WPS-PBC-Verfahren noch einmal durchführen. Weitere Informationen dazu finden Sie in der Kurzanleitung, die Sie zusammen mit dem CVE-30360 erhalten haben.

- Wenn Sie das WPS-PIN-Verfahren verwenden, bei dem Sie bei jedem Gerät im Netzwerk ein WPS-Passwort eingeben müssen, rufen Sie den Menüpunkt **Wireless** > **Grundeinstellungen** auf, und klicken Sie auf die Schaltfläche **PIN**. Geben Sie im nun erscheinenden Fenster die WPS-PIN, die Sie für den CVE-30360 verwenden möchten, oder die WPS-PIN des Client-Geräts, das Sie zum Netzwerk hinzufügen möchten, ein.
- Wenn Sie WEP verwenden, rufen Sie den Menüpunkt **Wireless** > **Sicherheit** auf. Im Abschnitt **WEP-Einstellungen** können Sie die Schlüssel festlegen, die Sie verwenden möchten. Klicken Sie abschließend auf **Übernehmen**.
- Wenn Sie WPA-PSK oder WPA2-PSK verwenden, rufen Sie den Menüpunkt **Wireless** > **Sicherheit** auf. Geben Sie bei **WPA_Personal** im Feld **PSK** das neue Passwort ein. Klicken Sie abschließend auf **Übernehmen**.

Unabhängig von der Wahl des Sicherheitsverfahrens: Wenn Sie das Passwort am CVE-30360 ändern, können die anderen Geräte nur dann eine Verbindung zum Netzwerk herstellen, wenn auch bei ihnen das Passwort geändert wurde.

Wie Sie das Passwort an den Client-Geräten ändern, ist abhängig vom Hersteller und vom Modell. Normalerweise müssen Sie sich im Konfigurationsprogramm des Geräts anmelden, und dann ähnlich wie beim CVE-30360 vorgehen. Nur beim WPS-PBC-Verfahren müssen Sie lediglich auf die WPS-Taste des CVE-30360 drücken und dann innerhalb von zwei Minuten danach auf die WPS-Tasten der anderen Geräte.

HINWEIS: Wenn Sie das WPS-PBC-Verfahren verwenden müssen Sie sich darüber im Klaren sein, dass alle Geräte, die WPS unterstützen, innerhalb dieser Verbindungszeit die Verbindung zum CVE-30360 herstellen können. Es ist also kein geeignetes Verfahren für öffentliche Bereiche oder wenn Sie den Verdacht haben, dass Unbefugte versuchen, auf das Netzwerk zuzugreifen.

5.2.3 ÄNDERN DES NETZWERKNAMENS (SSID)

Wenn Sie die SSID (der Name, der angezeigt wird, wenn Sie mit Ihrem Wireless Client nach Drahtlosnetzwerken suchen) Ihres Drahtlosnetzwerks ändern möchten, rufen Sie das Fenster **Wireless** > **Grundeinstellungen** auf. Geben Sie den Netzwerknamen in das Feld **SSID-Name** ein, und klicken Sie auf **Übernehmen**.

HINWEIS: Da die SSID für die Verbindung zu einem Netzwerk erforderlich ist, müssen Sie mit den Client-Geräte eine neue Verbindung mit der neuen SSID herstellen.

5.2.4 VERBERGEN DES NETZWERKS

Es gibt zahlreiche Gründe dafür, ein Netzwerk für Personen unsichtbar zu machen, die nach verfügbaren drahtlosen Netzwerken suchen. Rufen Sie dazu den Menüpunkt **Wireless** > **Grundeinstellungen** auf. Markieren Sie das Kontrollkästchen **verborgen**, und klicken Sie auf **Übernehmen**.

5.2.5 VERBESSERN DER LEISTUNG DES DRAHTLOSNETZWERKS

Zwei Hauptfaktoren können sich auf die Kommunikation Ihrer Drahtlosgeräte auswirken:

1. Störungen durch physische Objekte
2. Hochfrequenz-Störungen (HF)

So können Sie Störungen durch physische Objekte minimieren:

- Vergrößern Sie den Abstand vom CVE-30360 zu Wänden, schweren Möbeln oder massiven oder metallischen Gegenständen wie Kühlschränken usw.
- Installieren Sie den CVE-30360 in einer höher gelegenen Position.

So können Sie Hochfrequenz-Störungen minimieren:

- Entfernen Sie den Abstand vom CVE-30360 zu Hochfrequenzenergiequellen wie der Basisstation von Schnurlostelefonen, Mikrowellengeräten usw.
- Prüfen Sie vor Ort, ob andere Netzwerk mit Ihrem Netzwerk Störungen verursachen. Ist das der Fall, können Sie für die Drahtlosverbindung einen weniger belegten Kanal verwenden.

  Um diese Vor-Ort-Prüfung am CVE-30360 durchzuführen, rufen Sie den Menüpunkt **Wireless** > **WiFi Site Survey** auf. Klicken Sie auf **Scan**. Die jetzt erscheinende Maske zeigt die Drahtlosnetzwerke der Umgebung an. Im Feld **ch** ist zu sehen, welcher Kanal verwendet wird, und im Feld **signal (%)** wird angezeigt, wie stark der CVE-30360 das Signal empfängt (beachten Sie, dass die Stärke eines Netzwerks am CVE-30360 nicht unbedingt der Stärke desselben Netzwerks an der Position des Wireless Clients entspricht, dort kann das Signal viel stärker sein).

  Verwenden sehr viele Netzwerke oder ein sehr starkes Netzwerk einen Kanal oder eine Gruppe von Kanälen, können Sie den CVE-30360 auf einen weiter entfernten Kanal verlegen. Wenn Sie den CVE-30360 auf einen anderen Kanal legen möchten, rufen Sie den Menüpunkt **Wireless** > **Grundeinstellungen** auf, und wählen Sie eine Option aus der **Channel**-Liste aus. Wählen Sie einen Kanal aus, der so weit weg wie möglich vom belegten Bereich liegt. Ideal ist ein Abstand von fünf Kanälen.

  Je nach Konfiguration muss unter Umständen auch der Kanal an den Client-Geräten neu eingestellt werden.

5.3 ERWEITERTE DRAHTLOSNETZWERKFUNKTIONEN

In diesem Abschnitt erhalten Sie ausführlichere technische Informationen über Drahtlosnetzwerke.

HINWEIS: Dieser Abschnitt ist nicht erforderlich, wenn Sie das Drahtlosnetzwerk nur in einer Standardkonfiguration einrichten möchten (beschrieben unter Anleitung zur Nutzung der Drahtlosfunktion auf Seite 59).

5.3.1 ERWEITERTE SICHERHEITSEINSTELLUNGEN IM DRAHTLOSNETZWERK

In diesem Abschnitt werden die vom CVE-30360 unterstützten Sicherheitsprotokolle ausführlicher beschrieben.

- **WEP** (Wired Equivalency Protocol): Dieses Protokoll verwendet eine Reihe von “Schlüsseln” oder Zeichenketten, um den Wireless Client am Zugriffspunkt zu authentifizieren und um Daten zu verschlüsseln, die über die Drahtlosverbindung gesendet werden. WEP ist ein veraltetes Protokoll, das nur verwendet werden sollte, wenn es der einzige Sicherheitsstandard ist, der von allen Wireless Clients unterstützt wird. WEP bietet nur eine geringe Sicherheit, da es vielfältige Programme gibt, die diesen Sicherheitsschlüssel in wenigen Minuten “knacken” können.
- **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA wurde entwickelt, um die Unzulänglichkeiten des WEP-Protokolls zu lösen. Es gibt zwei WPA-Typen: Für die “Unternehmens”-Version (auch bekannt als WPA) wird ein zentraler Authentifizierungs-Datenbankserver benötigt. Bei der “privaten” Version (vom CVE-30360 unterstützt) kann sich der Benutzer mit einem “PSK”-Schlüssel oder einem Passwort authentifizieren. Auch wenn WPA relativ sicher ist, kann es Angriffe durch “brute-force” Passwort-Raten (bei dem ein Angreifer den AP mit unzähligen verschiedenen Passwörtern “bombardiert”) nicht standhalten. Deshalb wird für eine optimale Sicherheit empfohlen, ein zufälliges Passwort zu wählen, das aus mindestens dreizehn Zeichen besteht und keine tatsächlich existierenden Wörter enthält.
- **WPA2-PSK**: WPA2 ist eine Weiterentwicklung von WPA. Der grundlegende Unterschied liegt darin, dass WPA den mit Schwachstellen behafteten TKIP-Verschlüsselungsstandard (Temporal Key Integrity Protocol) verwendet, während WPA2 den stärkeren AES-Standard (Advanced Encryption Standard) im CCMP-Protokoll nutzt. Dieser trägt das höchste Prüfsigel der US-Regierung für Kommunikationssicherheit. Da WPA2-PSK denselben PSK-Mechanismus wie WPA-PSK verwendet, treffen auch hier bei der Verwendung unsicherer oder einfacher Passwörter dieselben Vorbehalte zu.

5.3.2 SONSTIGE INFORMATIONEN ÜBER DRAHTLOSNETZWERKE

In diesem Abschnitt erhalten Sie weitergehende Informationen über Drahtlosnetzwerke.

5.3.2.1 WPS

WPS (WiFi-Protected Setup) ist ein standardisiertes Verfahren, mit dem sich Drahtlosgeräte bei sehr großer Sicherheit schnell und einfach mit Drahtlosnetzwerken verbinden können. Der CVE-30360 bietet zwei WPS-Authentifizierungsverfahren:

- **PBC (Push-Button Configuration)**: Wenn der Benutzer die **PBC**-Taste am AP (entweder eine physische Taste oder eine virtuelle Taste in der Benutzeroberfläche) drückt, kann jeder Benutzer eines Wireless Clients, der WPS unterstützt, innerhalb der zwei darauffolgenden Minuten ebenfalls auf die jeweilige **PBC**-Taste am Client drücken, um das Gerät mit dem Netzwerk zu verbinden.
- **PIN-Konfiguration (Personal Identification Number)**: Alle WPS-fähigen Geräte haben eine PIN (diese befindet sich normalerweise auf einem Etikett am Gehäuse des Geräts). Wenn Sie ein anderes Gerät so konfigurieren, dass es dieselbe PIN verwendet, können sich die zwei Geräte gegenseitig authentifizieren.

Nach der Authentifizierung verwenden Geräte, die sich mit WPS mit einem Netzwerk verbunden haben, den Sicherheitsstandard WPA2.

5.3.2.2 WMM

WMM (WiFi MultiMedia) ist eine QoS-Verbesserung (Quality of Service), durch die bestimmte Datentypen bei der Übertragung im Drahtlosnetzwerk priorisiert werden. WMM bietet vier Datentypenklassifizierungen (geordnet nach Priorität: von der höchsten zur niedrigsten):

- Sprache
- Video
- Best effort (Beste Bemühung)
- Hintergrund

Wenn Sie die Leistung von Ton und Bild verbessern möchten (auf Kosten anderer, weniger zeitkritischer Anwendungen wie Internetbrowsing und FTP-Übertragungen), können Sie WMM aktivieren. Sie können auch die WMM QoS-Parameter bearbeiten. Das sollten Sie aber nur tun, wenn es unbedingt nötig ist.

5.4 DIE EINGABEMASKEN FÜR DIE DRAHTLOSKONFIGURATION

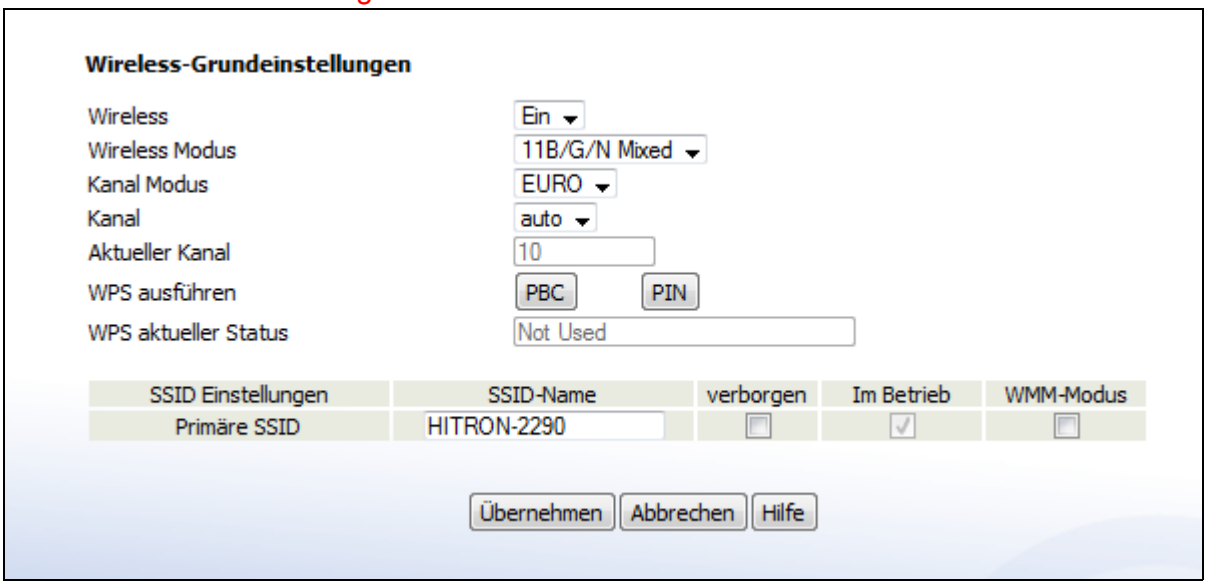
In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **Wireless** beschrieben.

5.4.1 DIE EINGABEMASKE WIRELESS-GRUNDEINSTELLUNGEN

In dieser Eingabemaske konfigurieren Sie die Grundeinstellungen für die Drahtlosverbindung des CVE-30360. Sie können das Drahtlosmodul ein- oder ausschalten, den Drahtlosmodus und Kanal auswählen, WPS ausführen und die SSID des Drahtlosnetzwerks konfigurieren.

Wenn Sie auf **Wireless** > **Basic** klicken, erscheint die folgende Eingabemaske.

ABBILDUNG 23: Die Eingabemaske Wireless > Basic



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 19: Die Eingabemaske Wireless > Basic

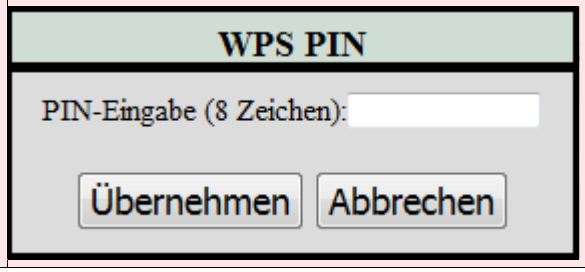
Wireless-Grundeinstellungen	
Wireless	In diesem Feld können Sie das Drahtlosnetzwerk ein- oder ausschalten. ▸ Wählen Sie **EIN**, um das Drahtlosnetzwerk einzuschalten. ▸ Wählen Sie **AUS**, um das Drahtlosnetzwerk auszuschalten.
Wireless Modus	Wählen Sie den Drahtlosnetzwerktyp, den Sie verwenden möchten: ▸ **11B/G Mixed**: IEEE 802.11b und 802.11n ▸ **11B Only**: IEEE 802.11b ▸ **11G Only**: IEEE 802.11g ▸ **11N Only**: IEEE 802.11n ▸ **11G/N Mixed**: IEEE 802.11g und 802.11N ▸ **11B/G/N Mixed**: IEEE 802.11b, 802.11g und 802.11N ***HINWEIS:*** Nur Wireless Clients, die das gewählte Netzwerkprotokoll unterstützen, können die Verbindung zum Drahtlosnetzwerk herstellen. Ist Ihnen das Protokoll nicht bekannt, sollten Sie **11B/G/N** (Standardeinstellung) verwenden.
Kanal	Wählen Sie den drahtlosen Kanal aus, der verwendet werden soll, oder wählen Sie **Auto**, damit der CVE-30360 automatisch den optimalen Kanal auswählt. ***HINWEIS:*** Es wird empfohlen, die Option **Auto** zu verwenden.
WPS ausführen	Mit diesen Tasten können Sie das Netzwerk mit der WPS-Funktion (Wifi Protected Setup) einrichten: ▸ Klicken Sie auf **PBC**, um die Tastenkonfiguration zu starten. Dann müssen Sie innerhalb der nächsten zwei Minuten auf die PBC-Taste der Wireless Clients drücken, damit diese im Drahtlosnetzwerk registriert werden. ▸ Klicken Sie auf **PIN**, um die PIN-Konfiguration zu starten. In der folgenden Eingabemaske geben Sie die WPS-PIN ein, die Sie für den CVE-30360 verwenden möchten, bzw. die WPS-PIN des Client-Geräts, das Sie zum Netzwerk hinzufügen möchten. ***ABBILDUNG 24:*** WPS PIN 

TABELLE 19: Die Eingabemaske Wireless > Basic

SSID Einstellungen	Hier wir die **Primäre SSID** angezeigt. *HINWEIS:* Je nach Vertragsumfang mit Ihrem Netzbetreiber können Sie auch weitere BSSIDs haben.
SSID-Name	Geben Sie den Namen ein, den Sie für das Drahtlosnetzwerk verwenden möchten. Dieser Name bezeichnet das Netzwerk, mit dem die Wireless Clients verbunden werden. *HINWEIS:* Aus Sicherheitsgründen wird empfohlen, die SSID zu ändern.
verborgen	Mit der Auswahl in diesem Feld können Sie das Netzwerk für andere Drahtlosgeräte sichtbar oder unsichtbar machen. ▶ Markieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass der CVE-30360 den Netzwerknamen (SSID) an alle Drahtlosgeräte sendet, die sich innerhalb der Reichweite befinden. Nur die Benutzer, die die SSID kennen, können die Verbindung zum Netzwerk herstellen. ▶ Entfernen Sie die Markierung, wenn Sie möchten, dass der Netzwerkname (SSID) öffentlich sichtbar ist. Alle Drahtlosgeräte, die sich innerhalb der Reichweite befinden, können die SSID erkennen und versuchen, die Verbindung zum Netzwerk herzustellen.
Im Betrieb	In diesem Feld wird bestimmt, ob die SSID verwendet wird oder nicht. *HINWEIS:* Zum Zeitpunkt der Druckstellung ist dieses Feld nicht vom Benutzer konfigurierbar.
WMM-Modus	Markieren Sie dieses Kontrollkästchen, wenn Sie die WMM QoS-Einstellungen (Wifi MultiMedia Quality of Service) auf diese SSID anwenden möchten.

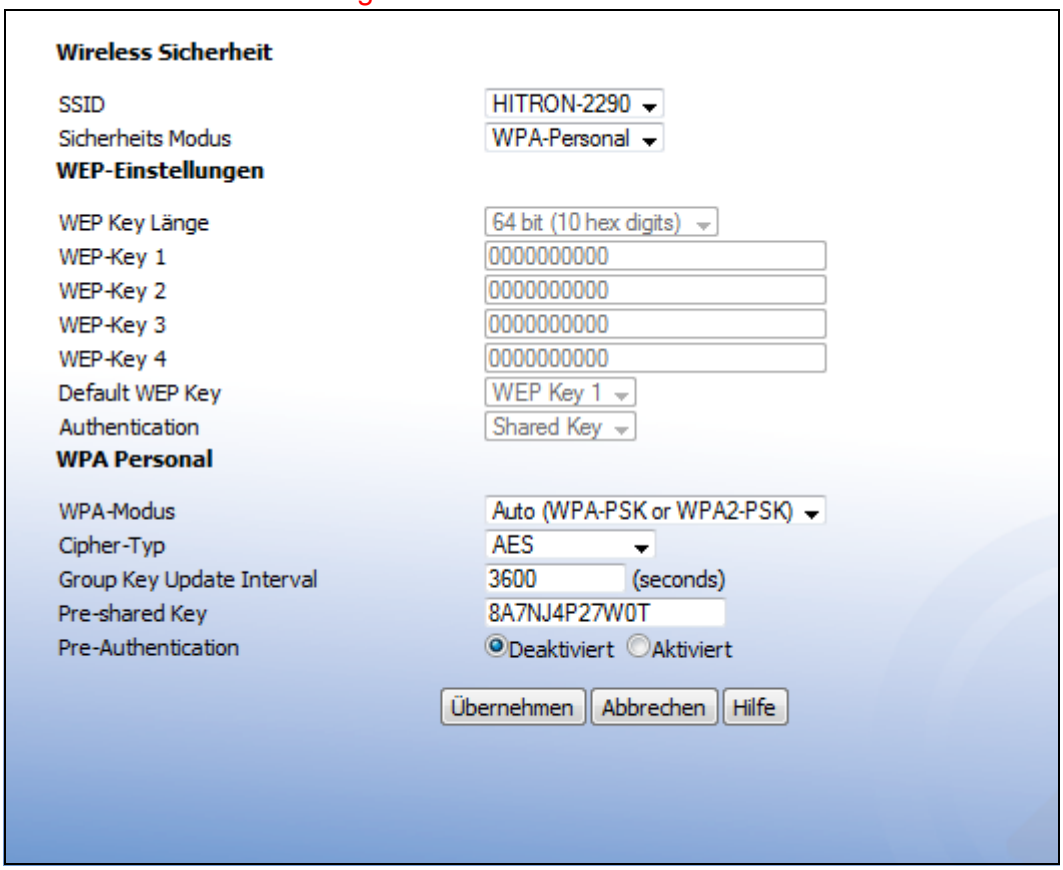
5.4.2 DIE EINGABEMASKE SICHERHEIT

In dieser Eingabemaske werden die Authentifizierung und Verschlüsselung des Drahtlosnetzwerks konfiguriert.

HINWEIS: Es wird dringend empfohlen, das Netzwerk zu sichern, da anderenfalls jeder auf das Netzwerk zugreifen kann, der sich innerhalb der Funkreichweite befindet.

Klicken Sie auf **Wireless** > **Sicherheit**. Das folgende Fenster erscheint.

ABBILDUNG 25: Die Eingabemaske Wireless > Sicherheit



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 20: Die Eingabemaske Wireless > Sicherheit

Wireless-Sicherheit	
SSID	Hier wählen Sie die SSID aus, für die Sie die Sicherheitseinstellungen vornehmen möchten. *HINWEIS:* Zum Zeitpunkt der Druckstellung ist nur eine SSID verfügbar.
Sicherheits Modus	Wählen Sie den Sicherheitstyp, den Sie verwenden möchten: ▶ Wählen Sie **None**, wenn Sie keine Sicherheit konfigurieren möchten. Jeder, der sich innerhalb der Reichweite befindet, kann auf das Netzwerk zugreifen. ▶ Wählen Sie **WEP**, um das Sicherheitsprotokoll Wired Equivalent Privacy (WEP) zu verwenden. ▶ Wählen Sie **WPA-Personal**, um das Sicherheitsprotokoll WiFi Protected Access (Personal) (WPA-Personal) zu verwenden. *HINWEIS:* **WEP** sollten Sie aufgrund seiner Unzulänglichkeiten nur verwenden, wenn dieses das einzige Sicherheitsprotokoll ist, dass alle Wireless Clients unterstützen. Sofern es möglich ist, sollten Sie unbedingt **WPA-Personal** verwenden.

TABELLE 20: Die Eingabemaske Wireless > Sicherheit (Fortsetzung)

WEP-Einstellungen *HINWEIS:* Diese Felder sind nur konfigurierbar, wenn Sie in der Liste **Sicherheits Modus** die Option **WEP** ausgewählt haben.	
WEP Key Länge	In diesem Feld legen Sie die Länge des Sicherheitsschlüssels fest, mit dem die Drahtlosgeräte Zugriff auf das Netzwerk erhalten. Je länger der Schlüssel ist, um so sicherer ist er. ▸ Wählen Sie **64-bit**, um einen zehnstelligen Sicherheitsschlüssel zu verwenden. ▸ Wählen Sie **128-bit**, um einen sechsundzwanzigstelligen Sicherheitsschlüssel zu verwenden.
WEP-Key 1-4	In diesen Feldern legen Sie die Sicherheitsschlüssel fest, die alle Drahtlosgeräte des Netzwerks verwenden müssen, um auf das Netzwerk zugreifen zu können. Der CVE-30360 unterstützt bis zu vier WEP-Schlüssel, von denen Sie einen als Standardschlüssel festlegen können. In den Wireless Clients des Netzwerks müssen dieselben vier Schlüssel in derselben Reihenfolge eingegeben werden. Der CVE-30360 und die Wireless Clients können unterschiedliche Standardschlüssel verwenden, solange alle vier Schlüssel in der richtigen Reihenfolge vorhanden sind. Wenn Ihr Wireless Client nur einen einzigen WEP-Schlüssel unterstützt, müssen Sie den Standardschlüssel des CVE-30360 verwenden. Geben Sie die Schlüssel im Hexadezimalformat (mit den Ziffern **0**-**9** und den Buchstaben **A**-**F**) ein.
Default WEP Key	Wählen Sie die Nummer des Sicherheitsschlüssels, den der CVE-30360 als Standardschlüssel zum Authentifizieren der Übertragungen verwenden soll.
Authentication	Wählen Sie einen Authentifizierungsmodus aus: ▸ Wählen Sie **Open System**, müssen sich die Wireless Clients zunächst vor dem CVE-30360 authentifizieren (legitimieren), bevor sie die Sicherheitsdaten (WEP-Schlüssel) vorweisen. ▸ Wählen Sie **Shared Key**, wird für die Authentifizierung der WEP-Schlüssel verwendet. Wenn ein Client die Verbindung zum Netzwerk herstellen möchten, sendet der CVE-30360 eine unverschlüsselte Abfragenachricht. Der Client muss die Abfragenachricht mit dem WEP-Schlüssel verschlüsseln und zum CVE-30360 zurücksenden. Dieser entschlüsselt diese Nachricht und vergleicht das Ergebnis mit der Ursprungsnachricht. Die **Open System**-Authentifizierung ist der sicherere dieser zwei Authentifizierungstypen. Obwohl das **Shared Key**-System auf den ersten Blick sehr widerstandfähig wirkt, können die Daten der Abfragenachrichten abgefangen werden. ▸ Wenn Sie **Auto** wählen, wählt der CVE-30360 das Authentifizierungsverfahren automatisch.

TABELLE 20: Die Eingabemaske Wireless > Sicherheit (Fortsetzung)

WPA_Personal *HINWEIS:* Diese Felder sind nur konfigurierbar, wenn sie in der Liste **Sicherheits Modus** die Option **WPA-Personal** ausgewählt haben.	
WPA-Modus	Wählen Sie einen WPA-Sicherheitstyp: ▶ Wählen Sie **WPA-PSK**, um den WPA-PSK-Modus (Wifi Protected Access (Pre-Shared Key)) zu verwenden. ▶ Wählen Sie **WPA2-PSK**, um den WPA2-PSK-Modus (Wifi Protected Access 2 (Pre-Shared Key)) zu verwenden. ▶ Wählen Sie **Auto (WPA-PSK oder WPA2-PSK)**, damit alle Clients unabhängig vom Modus die Verbindung zum CVE-30360 herstellen können.
Cipher Typ	Wählen Sie einen Verschlüsselungstyp: ▶ Wählen Sie **TKIP**, um das TKIP-Protokoll (Temporal Key Integrity Protocol) zu verwenden. ▶ Wählen Sie AES, um den AES-Standard (Advanced Encryption Standard) zu verwenden. ▶ Wenn Sie TKIP und AES wählen, können die Clients eine der beiden Verschlüsselungstypen verwenden, wenn Sie die Verbindung zum CVE-30360 herstellen möchten.
Group Key Update Interval	Geben Sie die Frequenz (in Sekunden) ein, mit der der CVE-30360 neue PSK-Schlüssel erzeugen und an die Wireless Clients ausgeben soll.
PSK	Geben Sie den PSK ein, den Sie für das Drahtlosnetzwerk verwenden möchten. Sie müssen diesen Schlüssel bei Ihren Wireless Clients eingeben, damit diese eine Verbindung zum Netzwerk herstellen können.
Pre-Authentication	In diesem Feld können Sie bei WPA2 eine Vor-Authentifizierung zulassen (**Aktiviert**) oder Vor-Authentifizierungsanfragen abweisen (**Deaktiviert**). Bei der Vor-Authentifizierung kann ein Wireless Client mit WPA2 eine Authentifizierung mit anderen drahtlosen Zugriffspunkten durchführen, die sich innerhalb der Reichweite befinden, auch wenn er immer noch mit dem aktuellen drahtlosen Zugriffspunkt verbunden ist. Auf diese Weise können mobile Wireless Clients für ein effizienteres Roaming schneller auf Zugriffspunkte zugreifen.
Übernehmen	Klicken Sie hier, um die Änderungen in diesem Fenster zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieses Fensters.

5.4.3 DIE EINGABEMASKE ZUGANGS KONTROLLE

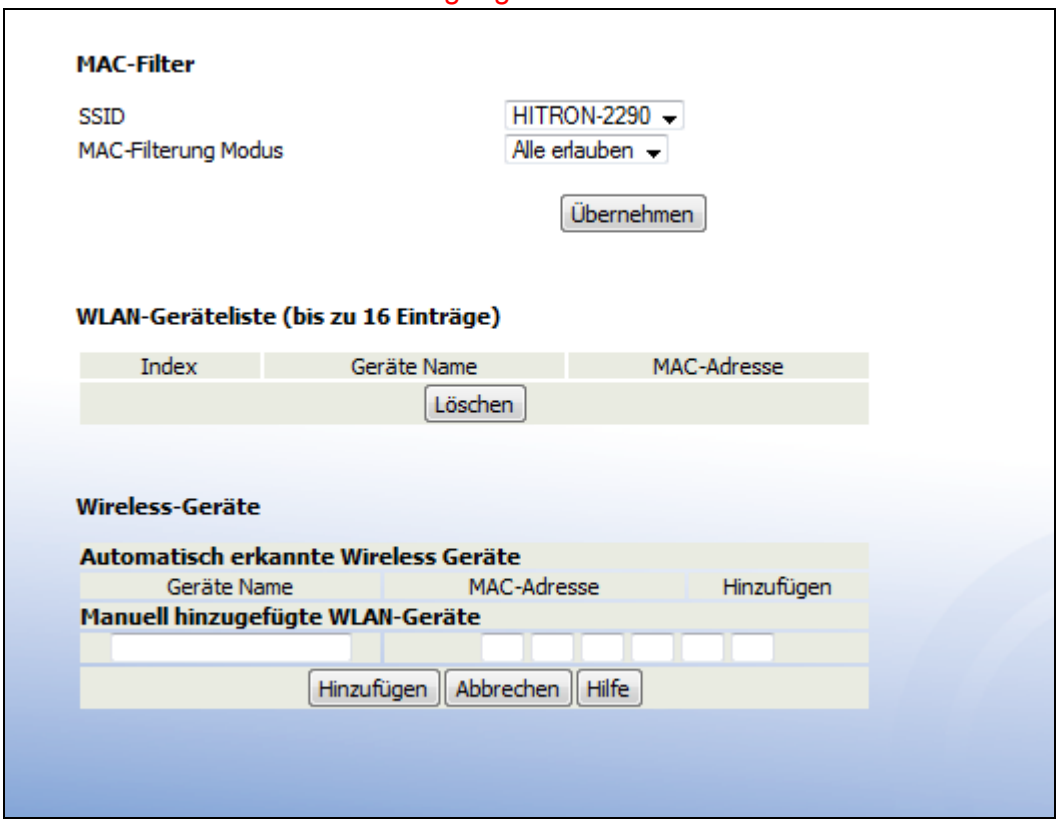
In diesem Fenster konfigurieren Sie die MAC-Adressfilterfunktion im Drahtlosnetzwerk.

HINWEIS: Eine Beschreibung, wie der MAC-Adressfilter im kabelgebundenen LAN konfiguriert wird, finden Sie unter Die Eingabemaske MAC-Filter auf Seite 44.

Sie können den CVE-30360 so einstellen, dass er nur bestimmten Geräten den drahtlosen Zugriff zum CVE-30360 und zum Netzwerk gewährt, diesen aber anderen Geräten verweigert.

Klicken Sie auf **Wireless** > **Zugangs Kontrolle**. Das folgende Fenster erscheint.

ABBILDUNG 26: Wireless > Zugangs Kontrolle.



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in diesem Fenster.

TABELLE 21: Das Fenster Wireless > Zugangs Kontrolle

MAC-Filter	
SSID	Wählen Sie die SSID, für die Sie die drahtlose Zugriffssteuerung konfigurieren möchten. *HINWEIS:* Zum Zeitpunkt der Drucklegung unterstützt der CVE-30360 nur eine einzige SSID.

TABELLE 21: Das Fenster Wireless > Zugangs Kontrolle (Fortsetzung)

MAC-Filterung Modus	In diesem Feld können Sie festlegen, ob der CVE-30360 im Drahtlosnetzwerk einen MAC-Filter anwendet. ▸ Wählen Sie **Alle erlauben**, um den MAC-Filter auszuschalten. Alle Geräte können auf den CVE-30360 und auf das Netzwerk zugreifen. ▸ Wählen Sie **Erlauben**, damit nur Geräte, deren MAC-Adresse sich in der **WLAN-Geräteliste** befinden, auf den CVE-30360 und das Netzwerk drahtlos zugreifen können. Allen anderen Geräten wird der Zugriff verwehrt. ▸ Wenn Sie **Verbieten** wählen, erhalten alle Geräte den drahtlosen Zugriff auf den CVE-30360 und auf das Netzwerk. Ausgenommen sind die Geräte, deren MAC-Adresse in der **WLAN-Geräteliste** steht. Den angegebenen Geräten wird der Zugriff verweigert.
Übernehmen	Klicken Sie hier, um die Änderungen im Abschnitt MAC-Filter zu speichern.
WLAN-Geräteliste (bis zu 16 Einträge)	
Index	Hier wird die Indexnummer des Drahtlosgeräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
Geräte Name	Hier wird der Name des Geräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
MAC-Adresse	Hier wird die MAC-Adresse des Geräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
Löschen	Wählen Sie die Optionsschaltfläche ( ) eines zugelassenen oder verweigerten Geräts aus der Liste. Dieses Gerät kann dann nicht mehr auf den CVE-30360 und das Netzwerk zugreifen.
Automatisch erkannte Wireless Geräte	
Geräte Name	Hier wird der Name aller Netzwerkgeräte angezeigt, die im Drahtlosnetzwerk mit dem CVE-30360 verbunden sind.
MAC-Adresse	Hier wird die MAC-Adresse aller Netzwerkgeräte angezeigt, die im Drahtlosnetzwerk mit dem CVE-30360 verbunden sind.
Manuell hinzugefügte WLAN-Geräte	
Geräte Name	Geben Sie den Namen des Geräts ein, dem der drahtlose Zugriff zum CVE-30360 und zum Netzwerk gewährt oder verweigert werden soll. ***HINWEIS:*** Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
MAC-Adresse	Geben Sie die MAC-Adresse des Netzwerkgeräts ein, für das Sie den drahtlosen Zugriff auf den CVE-30360 und das Netzwerk zulassen oder verweigern möchten.

TABELLE 21: Das Fenster Wireless > Zugangs Kontrolle (Fortsetzung)

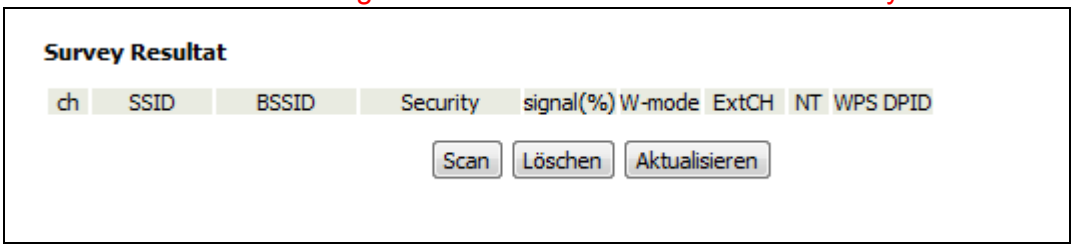
Hinzufügen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

5.4.4 DIE EINGABEMASKE WI-FI SITE SURVEY

In dieser Eingabemaske werden Informationen über die Drahtlosnetzwerke innerhalb der Reichweite des CVE-30360 angezeigt.

Wenn Sie auf **Wireless** > **Wi-Fi Site Survey** klicken, erscheint die folgende Eingabemaske.

ABBILDUNG 27: Die Eingabemaske Wireless > Wi-Fi Site Survey



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 22: Die Eingabemaske Wireless > Wi-Fi Site Survey

Survey Resultat	
ch	Hier wird die Nummer des Funkkanals angezeigt, welchen das Drahtlosnetzwerk verwendet.
SSID	In diesem Feld wird die SSID des Drahtlosnetzwerks angezeigt.
BSSID	In diesem Feld wird die BSSID des Drahtlosnetzwerks angezeigt. Das ist normalerweise die MAC-Adresse des Drahtlosnetzwerks.
Security	In diesem Feld wird der Sicherheitstyp angezeigt, den das Drahtlosnetzwerk verwendet.
signal (%)	In diesem Feld wird die Signalstärke des Drahtlosnetzwerks angezeigt, wie sie vom CVE-30360 das Drahtlossignal empfängt. Die Signalstärke wird in Prozent als Wert zwischen 0 (kein Empfang) und 100 (hervorragender Empfang) dargestellt.
W-mode	In diesem Feld wird der Netzwerkstandard (z. B. 11n) angezeigt, den das Drahtlosnetzwerk verwendet.

TABELLE 22: Die Eingabemaske Wireless > Wi-Fi Site Survey (Fortsetzung)

ExtCH	Bei IEEE 802.11n-Netzwerken, die drahtlose Übertragungen mit 40 MHz unterstützen, wird in diesem Feld angezeigt, ob das Netzwerk Kanäle bündelt. Gleichzeitig wird angegeben, ob der erweiterte Kanal über oder unter dem primären Steuerkanal liegt. ***HINWEIS:*** Mit der Kanalbündelung kann der Zugriffspunkt den Datendurchsatz durch die gleichzeitige Verwendung zweier Drahtloskanäle anstelle nur eines Kanals erhöhen. Wenn Sie die Kanalbündelung wählen, gibt es einen primären Steuerungskanal und einen Erweiterungskanal. Der Erweiterungskanal kann entweder direkt über dem Steuerungskanal liegen oder direkt darunter. ▶ Bei IEEE 802.11n-Netzwerken, die die Kanalbündelung verwenden, befindet sich der Erweiterungskanal über dem Hauptkanal, es erscheint **ABOVE**. ▶ Bei IEEE 802.11n-Netzwerken, die die Kanalbündelung verwenden, befindet sich der Erweiterungskanal unter dem Hauptkanal, es erscheint **BELOW**. ▶ Bei Netzwerken, die keine Kanalbündelung verwenden, erscheint **NONE**.
NT	In diesem Feld wird angezeigt, ob das Netzwerk den Infrastruktur- oder den Ad-Hoc-Modus verwendet. ***HINWEIS:*** Im Infrastrukturmodus verbinden sich die Drahtlosgeräte mit einem zentralen Zugriffspunkt (AP), der dann über eine Kabelverbindung die Verbindung zum Internet oder einem anderen Netzwerk herstellt. Im Ad-Hoc-Modus verbinden sich die Drahtlosgeräte als Peers miteinander.
WPS DPID	In diesem Feld wird angezeigt, ob das Zielnetzwerk WPS (WiFi Protected Setup) verwendet. Ist das der Fall, steht in diesem Feld, ob es den PIN-Modus oder den PBC-Modus verwendet. ▶ Verwendet das Zielnetzwerk nicht WPS, erscheint **NO**. ▶ Verwendet das Zielnetzwerk WPS, und lässt es zu, dass Drahtlosgeräte die Verbindung mit dem PIN-Modus herstellen, erscheint **PIN**. ▶ Verwendet das Zielnetzwerk WPS, und lässt es zu, dass Drahtlosgeräte die Verbindung mit dem PBC-Modus herstellen, erscheint **PBC Mode**. ***HINWEIS:*** Weitere Informationen zu WPS und zum Unterschied zwischen dem PIN- und PBC-Modus finden Sie unter WPS auf Seite 63.

6 EMTA

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **EMTA** klicken. Diese Masken enthalten Informationen über das integrierte Multimedia Terminal Adapter-Modul des CVE-30360.

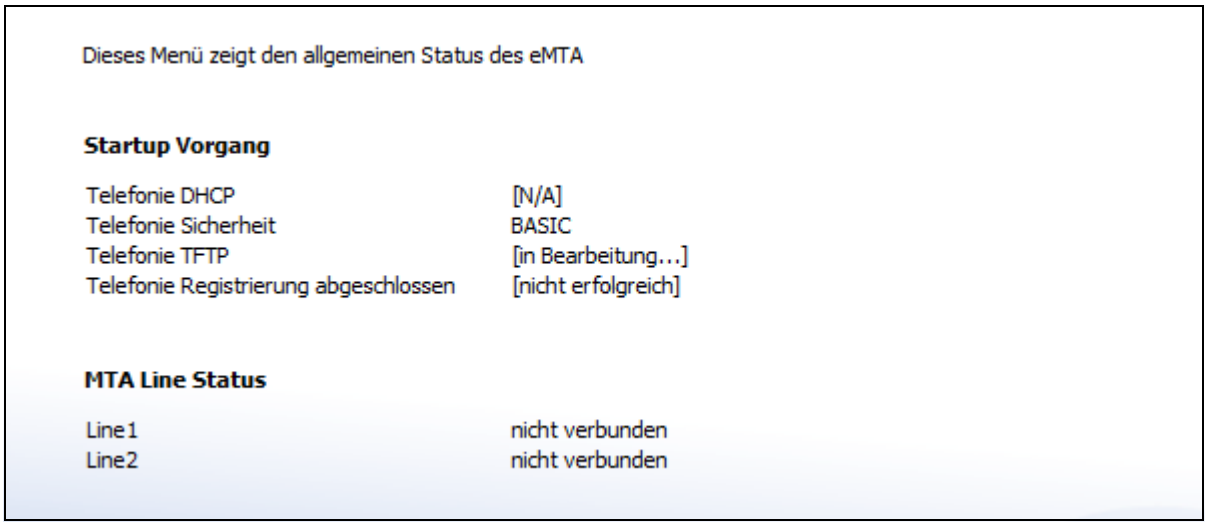
HINWEIS: Die Felder in diesen Masken sind schreibgeschützt und können lediglich zur Fehlerbehebung zu Rate gezogen werden.

6.1 DIE EINGABEMASKE STATUS

Diese Maske enthält allgemeine Informationen über das eMTA-Modul.

Klicken Sie auf **EMTA** > **Status**. Die folgende Eingabemaske erscheint.

ABBILDUNG 28: Die Maske EMTA > Status



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

TABELLE 23: Die Maske EMTA > Status

Startvorgang	
Telefonie DHCP	Dieses Feld zeigt den Status des Telefonie-DHCP-Remoteservers.
Telefonie Sicherheit	Hier wird der für Sprachanrufe über den CVE-30360 verwendete Sicherheitstyp angezeigt.

TABELLE 23: Die Maske EMTA > Status (Fortsetzung)

Telefonie TFTP	Dieses Feld zeigt den Status des Telefonie-TFTP-Remoteservers.
Telefonie-Registrierung beim Anrufserver	In diesem Feld wird der Verbindungsstatus zwischen allen Telefonleitungen des CVE-30360 und dem Remote-Anrufservers angezeigt.
Telefonie Registrierung abgeschlossen	In diesem Feld wird der Gesamtstatus der Sprachanrufregistrierung angezeigt.
SIP-Registrierung-Status	
SIP-Registrierung Timer	In diesem Feld wird die Zeit (in Sekunden) angezeigt, nach der sich der CVE-30360 neu beim SIP-Server (Session Initiation Protocol) registriert. Dieses Feld erscheint nicht, wenn der CVE-30360 nicht mit einem SIP-Server verbunden ist.
MTA Line Status	
Line 1	Diese Felder zeigen den aktuellen Status jedes am CVE-30360 angeschlossenen Telefons an. Sie werden nicht angezeigt, wenn an den jeweiligen Ports keine Telefone angeschlossen sind.
Line 2	

7

FEHLERBEHEBUNG

Mit Hilfe dieses Abschnitts können Sie allgemeine Probleme mit dem CVE-30360 und Ihrem Netzwerk lösen.

Problem: Keine der LEDs leuchtet

Der CVE-30360 wird nicht mit Strom versorgt, oder das Gerät hat einen Fehler.

1. Stellen Sie sicher, dass Sie den richtigen Netzadapter verwenden.

Wenn Sie einen anderen Netzadapter verwenden als den, der im Lieferumfang des CVE-30360 enthalten war, kann der CVE-30360 beschädigt werden.

2. Stellen Sie sicher, dass der Netzadapter richtig an den CVE-30360 und an das Stromnetz angeschlossen ist.
3. Stellen Sie sicher, dass die Stromquelle einwandfrei funktioniert. Wechseln Sie kaputte Sicherungen aus, und setzen Sie alle ausgelösten Schutzschalter zurück.
4. Trennen Sie den Netzadapter vom Stromnetz und vom CVE-30360, und stellen Sie dann beide Verbindungen wieder her.
5. Wenn das Problem mit keinem der oben genannten Schritte behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Eine der LEDs leuchtet nicht wie erwartet

1. Lesen Sie noch einmal nach, wie die LED normalerweise leuchten müsste (siehe LEDs auf Seite 18).
2. Stellen Sie sicher, dass die Hardware des CVE-30360 richtig angeschlossen wurde. Sehen Sie sich dazu auch die Installations-Kurzanleitung noch einmal an.
3. Trennen Sie den Netzadapter vom CVE-30360, und schließen Sie ihn wieder an.
4. Wenn das Problem mit keinem der oben genannten Schritte behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Sie haben die IP-Adresse des CVE-30360 vergessen

1. Die LAN IP-Standardadresse des CVE-30360 ist **192.168.0.1**.
2. Sie können die Benutzeroberfläche desCVE-30360 aufrufen, indem Sie in einem an das LAN angeschlossenen Computer den LAN-Domain-Suffix in die Adresszeile Ihres Browsers eingeben. Der Standardsuffix der LAN-Domain ist **hitronhub.home**. Weitere Informationen dazu finden Sie unter Die Eingabemaske LAN IP auf Seite 34.
3. Abhängig von Ihrem Betriebssystem und Netzwerk können Sie auch die IP-Adresse des CVE-30360 mit Hilfe des Standard-Gateways des Computers herausfinden. Bei den meisten Windows-Computern müssen Sie dazu auf **Start** > **Ausführen** klicken. Geben Sie dann “cmd” und “ipconfig” ein. Beziehen Sie die IP-Adresse des **Standard-Gateways**, und geben Sie diese in die Adresszeile Ihres Browsers ein.
4. Wenn Sie weiterhin keinen Zugriff auf den CVE-30360 haben, müssen Sie den CVE-30360 zurücksetzen. Siehe Zurücksetzen des CVE-30360 auf Seite 23. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Eingabemaske SICHERUNGSKOPIE auf Seite 38).

Problem: Sie haben den Administrator-Benutzernamen oder das Passwort für den Zugriff auf den CVE-30360 vergessen

1. Der Standard-Benutzername ist **admin** und das Standard-Passwort ist **password**.
2. Wenn dieser Benutzername und das Passwort nicht funktionieren, müssen Sie den CVE-30360 auf seine Standardeinstellungen zurücksetzen. Siehe Zurücksetzen des CVE-30360 auf Seite 23. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Eingabemaske SICHERUNGSKOPIE auf Seite 38).

Problem: Sie haben keinen Zugriff auf den CVE-30360 oder das Internet

1. Stellen Sie sicher, dass Sie für den CVE-30360 die richtige IP-Adresse verwenden.
2. Prüfen Sie die Hardwareverbindungen in Ihrem Netzwerk, und stellen Sie sicher, dass die LEDs des CVE-30360 richtig leuchten (siehe LEDs auf Seite 18).
3. Stellen Sie sicher, dass sich der Computer im selben Subnetz befindet wie der CVE-30360 (siehe Einrichten der IP-Adresse auf Seite 20).
4. Wenn Sie versuchen, eine WLAN-Verbindung herzustellen, könnte das Problem bei der Drahtlosverbindung liegen. Schließen Sie das Gerät an den **LAN**-Port an.

5 Wenn das Problem mit den oben beschriebenen Schritten nicht behoben werden kann, muss der CVE-30360 zurückgesetzt werden. Siehe Zurücksetzen des CVE-30360 auf Seite 23. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Eingabemaske SICHERUNGSKOPIE auf Seite 38).

6 Wenn das Problem dadurch nicht behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Sie können nicht auf das Internet zugreifen, und die LED-Lampen DS und US blinken

Möglicherweise hat Ihr Internetdienstanbieter Ihren Internetzugriff deaktiviert. Prüfen Sie in der Maske **Kabel** > **System Info** das Feld Netzwerkzugriff (siehe Die Eingabemaske SYSTEM INFO auf Seite 25).

Problem: Sie können mit Ihrem Drahtlosgerät keine Verbindung herstellen

1 Stellen Sie sicher, dass das Drahtlosgerät richtig funktioniert und richtig konfiguriert ist. Lesen Sie dazu u. U. in der Dokumentation des Drahtlosgeräts nach.

2 Stellen Sie sicher, dass sich das Drahtlosgerät innerhalb der Sendereichweite des CVE-30360 befindet. Hindernisse (Wände, Fußböden, Bäume usw.) und elektrische Störungen (andere Funktransmitter, Mikrowellenöfen usw.) verringern die Signalqualität und die Sendereichweite des CVE-30360.

3 Stellen Sie sicher, dass der CVE-30360 und das Drahtlosgerät auf denselben Drahtlosmodus, dieselbe SSID (siehe DIE EINGABEMASKE WIRELESS-GRUNDEINSTELLUNGEN auf Seite 64) und dieselben Sicherheitseinstellungen (siehe Die Eingabemaske Sicherheit auf Seite 66) eingestellt sind.

4 Geben Sie alle Sicherheitsdaten (WEP-Schlüssel, WPA(2)-PSK-Passwort oder WPS PIN) noch einmal ein.

5 Wenn Sie die PBC-Funktion des WPS verwenden, stellen Sie sicher, dass Sie innerhalb von zwei Minuten, nachdem Sie auf die PBC-Taste des CVE-30360 gedrückt haben, die PBC-Taste des Drahtlosgeräts betätigen.

INDEX

Zahlen

802.11b/g/n 16, 58, 65

A

Access Point 15
Adresse, IP 20
Adresse, IP, lokal 21
Anmeldemaske 20
anmelden 22
AP 15
authentifizierung 68

B

Benutzername 78
Benutzername und Passwort 22
Benutzeroberfläche 15

C

CATV 16

D

Debugging 37
De-Militarized Zone 55
DHCP 16, 20, 21, 36
Diagnose 34
DMZ 55
DMZ De-Militarized Zone 16
DNS 34
DOCSIS 25
Dokumentkonventionen 4
Domain Name System 34
Domain-Suffix 34
drahtlos 57
drahtloser Zugriffspunkt 15
drahtlosnetzwerk standards 58
drahtlossicherheit 59, 66, 67
Drahtlossicherheit, wireless 16
DS 20

E

EMTA 75
ETH 19
Ethernet 16
Ethernetkabel 18
Ethernet-Port 21

F

Fast Ethernet 16
Fehlersuche 34
Firewall 41
Funkabdeckung 66

G

grafische Benutzeroberfläche (GUI) 15
GUI 15, 23
GUI Übersicht 23

H

Hardware 16
Hauptfenster, Haupteingabemaske 23
HF-Anschluss 16
HF-Stecker 16

I

ICMP 42
IEEE 802.11b/g/n 16, 58
Intrusion Detection 42
Intrusion-Detection 16
IP Standardadresse 21
IP-Adresse 20, 21, 33, 78
IP-Adresse einrichten 21
IP-Adresse Setup 20
IP-Adresse, lokal 21
IP-Adresse, Standard 21
IP-Filter 16, 42, 46

K

Kabelmodem 15
Kabelverbindung 15
Kabelverbindungsstatus 27
Kindersicherung 16
Konto, anmelden 22
Konventionen, Dokument 4
Kundenbetreuung 4

L

Lampen 18
LAN 15, 33, 57
LAN 1-4 18
LAN IP 34
LEDs 18, 77, 79
Leiste, Navigation 23
Leitung 1-2 19
Local Area Network 15
Login-Konten 22
lokale IP-Adresse 21

M

MAC-adressfilter 70
MAC-Filter 16, 41, 44
Maske, Eingabemaske 15
MIMO 16
modem 15
Multiple-In, Multiple-Out 16

N

Navigation 23
Navigationsleiste 23
Netzwerk, Lokal 15
Netzwerk, Wide Area 15
Netzwerk, Wireless 15
Netzwerkdiagnose 34
Netzwerkgeräte, angeschlossen 27
Neustart 38

O

Open-System-Authentifizierung 68

P

Passwort 30, 78
Passwort und Benutzername 22
PBC konfiguration 63
PIN konfiguration 63
Ping 16, 34, 37, 41, 42
PIN-Konfiguration 16
Port, Ethernet 21
Ports 16
Port-Triggering 16, 53
Portweiterleitung 16, 42, 49
Pre-Authentifizierung 69
Pre-Shared-Key 69
programmierte Website-Sperre 16
Pushbutton-Konfiguration 16

Q

QoS 64

R

radio links 57
Regel, IP-Filter 48
Regel, Portweiterleitung 51
RJ45-Anschlüsse 18
Routing-Modus 33

S

Schaltflächen 16
Service Set 58
Shared-Key-Authentifizierung 68
Sicherheit 66, 67
Sichern 38
sprachgesteuertes Kabelmodem 15
SSID 58, 64
Standard 30, 38
Standard-Benutzername und Passwort 22
Standardeinstellung 17, 23
Standardeinstellungen 30, 38
Standardwerte 38
Stärke 18
Status 20, 27
Status, Kabelverbindung 27
Subnetz 20, 21, 33
Subnetz, IP 20
Support, Kunde 4
Switch-Setup 37

T

TCP/IP 21
Traceroute 16, 34, 37
Triggering, Port 16, 53
Typ F 16

U

Übersicht, GUI 23
US 20

V

Verbindungsprozess 27
Verbindungsstatus, Kabel 27
verbundene Netzwerkgeräte 27
verschlüsselungstyp 69
VoIP (Voice over IP) 16

W

WAN 15
WAN-Verbindung 27
Weiterleitung, Port 16, 42, 49
WEP 16, 59
Wide Area Network 15
Wifi MultiMedia 64
Wifi Protected Setup 16, 63
Windows XP 21
Wired Security 16
Wireless 57
Wireless Local Area Network 15
Wireless Security 16
Wireless-Einstellungen,
Grundeinstellungenn 64
Wireless-Netzwerkstandards 58
Wireless-Sicherheit 59, 67
Wirelessverbindung 79
WLAN 15, 57
WMM 64
WPA2 63
WPA2-PSK 16, 59
WPA-PSK 16, 59
WPS 16, 63, 64, 67
WPS PBC 17

X

XP, Windows 21

Z

zugriffssteuerung 70
zurücksetzen 17, 23